Command Reference for Cisco NCS 4000 Series

First Published: 2015-05-25

Last Modified: 2023-04-28

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

© 2022 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

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

This section provides the following information:

Document Objectives

This guide describes the various commands available to configure and maintain the Cisco NCS 4000 Series.

Audience

The Cisco command reference documentation set is intended primarily for users who configure and maintain Cisco networking devices (such as switches) but who may not be familiar with the tasks or the Cisco IOS XR commands necessary to perform particular tasks. This document also helps to know about the features and configuration options in the Cisco NCS 4000 Series.

Document Organization

This document is organized into the following chapters:

Chapter	Description
Optics Command Reference, on page 1	This chapter describes the command to create a controller use the port-mode command in the config mode.
Ethernet Controller Command Reference, on page 11	This chapter describes the command to configure the ethernet controller in the config mode.

Chapter	Description
Controllers OCn Command Reference, on page 15	This chapter describes the commands to configure the OCn controller in the config mode.
Controllers STSn Command Reference, on page 23	This chapter describes the commands to configure the STSn controller in the config mode.
Controllers STMn Command Reference, on page 31	This chapter describes the commands to configure the STMn controller in the config mode.
Controllers VCn Command Reference, on page 39	This chapter describes the commands to configure the VCn controller in the config mode.
ODU Controller Command Reference, on page 45	This chapter describes the commands to configure the ODUk controllers.
OTU Controller Command Reference, on page 67	This chapter describes the commands to configure the OTUk controllers.
Interface GCC Command Reference, on page 93	This chapter describes the commands to configure the interface gcc for ODUk and OTUk controllers.
Protection Command Reference, on page 101	This chapter describes the commands to protect the OTN controllers.
Cross Connect Command Reference, on page 117	This chapter describes the commands to create cross connection between the controllers.
GMPLS Command Reference, on page 121	This chapter describes the commands to configure GMPLS.
PRBS Command Reference, on page 167	This chapter provides the IOS XR commands to configure PRBS.
Controllers Breakout Command Reference, on page 171	This chapter provides the IOS XR commands to configure breakout.
Patch Cord Command Reference, on page 181	This chapter provides the IOS XR commands to configure patch cords between ports.
Frequency Synchronization Commands, on page 185	This chapter provides the IOS XR commands to configure Frequency Synchronization.
IPv4/OSPF Commands, on page 219	This chapter provides the IOS XR commands to configure Open Shortest Path First (OSPF) routing protocol.
IS-IS Command Reference, on page 429	This chapter provides the IOS XR commands to configure Intermediate System-to-Intermediate System (IS-IS) protocol.
L2Xconnect/VLAN/EVC Command Reference, on page 575	This chapter provides the IOS XR commands to configure point-to-point Layer 2 (L2) connectivity on Cisco NCS 4000 Series routers.

Chapter	Description
CFM-EOAM Command Reference, on page 589	This chapter provides the IOS XR commands to configure the Ethernet OAM.
VPWS Command Reference, on page 753	This chapter provides the IOS XR commands to configure VPWS .
BGP Route Reflector Commands , on page 777	This chapter provides the IOS XR commands to configure Border Gateway Protocol Route Reflect (BGP RR) .
MPLS Traffic Engineering Commands , on page 833	This chapter provides the IOS XR comamnds to configure MPLS Traffic Engineering.
Bidirectional Forwarding Commands, on page 871	This chapter provides the IOS XR commands to configure Bidirectional Forwarding.
Ethernet Local Management Interface Commands, on page 893	This chapter provides the IOS XR commands to configure Ethernet Local Management Interface.
Inter-Rack Pairing Command Reference, on page 905	This chapter provides the IOS XR commands to configure Inter-Rack Pairing.
Smart Licensing Command Reference, on page 909	This chapter provides the IOS XR commands to configure smart licensing.
Call Home Command Reference, on page 919	This chapter provides the IOS XR commands to configure call home functionality.
Link Layer Discovery Protocol (LLDP) Command Reference, on page 977	This chapter provides the IOS XR commands to configure LLDP.

Related Documentation

Use this guide in conjunction with the following referenced publications:

- *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
- *Cisco Network Convergence System 4000 Series Unpacking, Moving, and Securing Guide*
- *Hardware Installation Guide for Cisco NCS 4000 Series*
- *Configuration guide for Cisco NCS 4000 Series*
- *Troubleshooting Guide for Cisco NCS 4000 Series*
- *TL1 Guide for Cisco NCS 4000 Series*
- *Cisco IOS XR System Error Message Reference Guide*

Document Conventions

OTN and DWDM Command Reference Guide for Cisco NCS 4000 Series 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 non-bold 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.
[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 non quoted 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.
R/S/I/P	*Rack/Slot/Instance/Port*

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.**

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! I**NSTRUCCIONES IMPORTANTES DE SEGURIDAD**

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

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

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

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

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

请保存这些安全性说明

警告 安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

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

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

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

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

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

GEM DISSE ANVISNINGER

تحذير إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في آخر 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

Preface

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

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

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

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

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

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

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

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

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

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

USCHOVAJTE SI TENTO NÁVOD

Preface

Optics Command Reference

This chapter describes the commands to configure the Optics controller.

controller optics

To configure optics controller use the **controller optics** command in the config mode.

controller optics *R/S/I/P*

Syntax Description

controller optics	Name of the controller
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to configure an optics controller.

```
RP/0/RP0:hostname (config)# controller optics 0/0/0/0
```

automatic-in-service controller

To configure AINS use the **automatic-in-service controller** command in the EXEC mode.

automatic-in-service controller *controller-name R/S/I/P* **hours** *x* **minutes** *y*

Syntax Description

controller-name	Name of the controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
x	Number of hours
y	Number of minutes

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure AINS for 15 minutes on an ODU2 controller.

```
RP/0/RP0:hostname # automatic-in-service controller odu2 0/6/0/2 hours 0 minutes 15
```

dwdm-carrier

To configure the wavelength, use the **dwdm-carrier** command in optics controller configuration mode.

dwdm-carrier 100MHz-grid frequency *frequency*

Syntax Description

dwdm-carrier 100MHz-grid frequency	Configures the wavelength in 100MHz (0.1GHz) grid spacing in accordance with ITU definition.
frequency	Specifies the frequency for the optics controller. In 100MHz grid spacing, enter the 7-digit frequency value in the range of 1911500–1961000. For example, enter 1913501 to specify 191.3501 THz.

Command Default

No wavelength is configured.

Command Modes

Optics controller

Command History

Release	Modification
6.5.33	This command was introduced.

Usage Guidelines

You must shut down the controller before you configure the controller or restore a saved configuration.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to configure the wavelength in 100MHz (0.1GHz) grid spacing in accordance with ITU definition.

```
RP/0/RP0:ios(config-Optics)#dwdm-carrier 100MHz-grid frequency 1960810
```

port-mode

To create a controller use the **port-mode** command in the config mode. To delete the port-mode, use the **no** form of this command.

port-mode {**sonet** | **sdh** | **ethernet** | **otn**} [**framing** *type* **mapping** *type*]

no port-mode {**sonet** | **sdh** | **ethernet** | **otn**} [**framing** *type* **mapping** *type*]

Syntax Description

port-mode sonet framing	Possible framing and mapping types: { opu1 mapping bmp | opu2 mapping [amp | bmp] }
port-mode sdh framing	Possible framing and mapping types: { opu1 mapping bmp | opu2 mapping [amp | bmp] }
port-mode otn framing	Possible framing and mapping types: { opu1 | opu1e | opu1f | opu2 | opu2e | opu2f | opu3 | opu3e1 | opu3e2 | opu4 | opuflex }
port-mode ethernet framing	Possible framing and mapping types: { opu0 mapping gmp | opu1e mapping bmp | opu2 mapping { GfpF | wis rate [OC192 | STM64] | GfpF-Ext } opu2e mapping bmp | opu3 mapping | opu3e1 mapping | opu3e2 mapping | opu4 mapping [gmp | GfpF] | opuflex mapping GfpF }

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to create ethernet.

```
RP/0/RP0:hostname (config)# controller optics 0/0/0/0
RP/0/RP0:hostname (config-optics)# port-mode ethernet framing opu0 mapping gmp
```

show controller optics

To display status and configuration information about the interfaces configured as optics controller on a specific node, use the **show controllers optics** command in XR EXEC mode.

show controller optics

show controller optics *R/S/I/P* [**dwdm-carrier-map flexi-grid**]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port of the controller.
dwdm-carrier-map	(only for trunk optics controllers) Displays the wavelength and channel mapping.
flexi-grid	(only for trunk optics controllers) Enables GMPLS UNI flexible grid channel spacing.

Command Modes

Exec mode

Command History

Release	Modification
6.5.33	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

The following example displays the wavelength and channel mapping with flexible grid channel spacing enabled.

```
RP/0/RP0:ios#show controller Optics0/0/0/11 dwdm-carrier-map flexi-grid
Mon Mar 20 07:12:36.764 UTC
DWDM Carrier Band:: OPTICS_C_BAND
Frequency range supported: 196.10000 THz ~ 191.30630 THz
DWDM Carrier Map table
-----------------------------------------------------
Channel G.694.1 Frequency Wavelength
index Ch Num (THz) (nm)
-----------------------------------------------------
1 480 196.10000 1528.773
-----------------------------------------------------
2 479 196.09380 1528.822
-----------------------------------------------------
3 478 196.08750 1528.871
-----------------------------------------------------
4 477 196.08130 1528.919
-----------------------------------------------------
```

```
5 476 196.07500 1528.968
----------------------------------------------------
6 475 196.06880 1529.017
----------------------------------------------------
7 474 196.06250 1529.066
----------------------------------------------------
8 473 196.05630 1529.114
----------------------------------------------------
9 472 196.05000 1529.163
----------------------------------------------------
10 471 196.04380 1529.212
----------------------------------------------------
11 470 196.03750 1529.261
----------------------------------------------------
12 469 196.03130 1529.309
----------------------------------------------------
13 468 196.02500 1529.358
----------------------------------------------------
14 467 196.01880 1529.407
----------------------------------------------------
15 466 196.01250 1529.456
----------------------------------------------------
16 465 196.00630 1529.504
--More--
```

show portmode

To display details of portmode, use the **show portmode** command in the exec mode.

show controllers optics *R/S/I/P* **portmode capability**

Syntax Description

optics	Name of the port.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
portmode	Port mode

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

The following example shows how to display port-mode capability .

```
RP/0/RP0:hostname # show controller optics 0/0/0/1 portmode capabilities
```

```
Portmode Information
-------------------------------------------------------------
Port_no          Portmode Type   Framing                 Mapping
PT type
1                Ethernet        OPU0 framing type       GMP mapping type
07 (PCS codeword transparent Ethernet mapping)
1                Sonet           OPU1 framing type       BMP mapping type
03 (Bit synchronous CBR mapping)
1                SDH             OPU1 framing type       BMP mapping type
03 (Bit synchronous CBR mapping)
1                OTN             OPU1 framing type       None mapping type
Traffic Dependent
```

```
RP/0/RP0:hostname # show controller optics 0/0/0/1 portmode configured
```

```
Portmode Information
-------------------------------------------------------------
```

```
Portmode type   Framing Mapping          PT type
OTN             OPU1 framing type       None mapping type       Traffic Dependent
```

Note Run *do show portmode* when command is executed in config mode.

Ethernet Controller Command Reference

This chapter describes the commands to configure the Ethernet controller.

controller ethernet

To configure ethernet controller use the **controller optics port-mode ethernet** command in the config mode.

controller optics *R/S/I/P* {**port-mode**} {**ethernet**} [**framing** *type* **mapping** *type*]

Syntax Description

controller optics	Name of the controller
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
port-mode	Port mode.
ethernet	Type of the controller.
framing	Framing for the port mode.
mapping	Mapping for the port mode.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
Ethernet	write

Example

The following example shows how to configure an ethernet controller.

```
RP/0/RP0:hostname (config)# controller optics 0/0/0/0
RP/0/RP0:hostname (config-optics)# port-mode ethernet framing opu0 mapping gmp
```

controller sonet

To configure an sonet controller, use the **controller** command in the config mode. To delete the controller, use the **no** form of this command.

controller optics *R/S/I/P*
port-mode sonet [**framing** *type* **mapping** *type*] [**wis** *rate*]
no port-mode sonet [**framing** *type* **mapping** *type*] [**rate** *type*]

Syntax Description

controller	Name of the controller.
optics	Name of the controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
port-mode	Port mode
sonet	Name of the controller.
framing	Framing for the port mode.
mapping	Mapping for the port mode.
rate	Rate for the port mode.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
Ethernet	write

Example

This example shows how to create sonet controller:

```
RP/0/RP0:hostname (config) # controller optics 0/0/0/1
RP/0/RP0:hostname (config-optics) # port-mode ethernet framing opu2 mapping wis rate oc192
RP/0/RP0:hostname (config-optics) # no port-mode ethernet framing opu2 mapping wis rate
oc192
```

show controller (ethernet)

To display all the details of an ethernet controller, use the **show controllers** command in the exec mode.

show controllers {**GigabitEthCtrlr** | **TenGigECtrlr** | **HundredGigECtrlr**} *R/S/I/P*

Syntax Description

GigabitEthCtrlr	Displays the 1 gigabit ethernet controller.
TenGigECtrlr	Displays the 10 gigabit ethernet controller.
HundredGigECtrlr	Displays the 100 gigabit ethernet controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
Ethernet	read

Example

This example shows how to display the details of the ethernet controller:

```
RP/0/RP0:hostname # show controllers GigabitEthCtrlr 0/11/0/0
```

Controllers OCn Command Reference

This chapter describes the commands to configure the OCn controller.

loopback

To configure loopback on an OCn controller, use the **loopback** command in the config mode. To delete the loopback, use the **no** form of this command.

loopback [**internal** | **line**]
no loopback [**internal** | **line**]

Syntax Description

internal	Configures a terminal loopback on an OCn controller
line	Configures a line loopback on an OCn controller

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the loopback on the ocn port:

```
RP/0/RP0:hostname (config)# controller oc48 0/0/0/1
RP/0/RP0:hostname (config-oc48)# loopback internal
```

overhead j0

To configure overhead value on an OCn controller, use the **overhead j0** command in the config mode. To delete the overhead value from a OCn controller, use the **no** form of this command.

overhead j0 {**expected** | **send**} [**16Bytes** | **1Byte**] *string*

no overhead j0 {**expected** | **send**} [**16Bytes** | **1Byte**] *string*

Syntax Description

OCn	Name of the controller. Following are the valid value of n: • OC48 • OC192
expected	Configures the expected trace identifier of the OCn controller.
send	Configures the transmit trace identifier of the OCn controller.
16Bytes	Configures the 16 bytes path trace for the OCn controller.
1Byte	Configures the 1 byte path trace for the OCn controller.
string	Enters the ACSII text for the OCn controller.

Command Default

0 stands byte mode

BER thresholds : SF=10e-3 SD=10e-6

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the overhead j0 value on the OC48 controller:

```
RP/0/RP0:hostname(config)# controller oc48 0/0/0/2
RP/0/RP0:hostname(config-oc48)# overhead j0 expected 1Byte 5
```

pm (oc)

To configure the pm parameters for OC controller, use the **pm ocn** command in the config mode. To delete the pm parameters, use the **no** form of this command.

pm [**15-min** | **24-hour**] { **ocn**} [**report** | **threshold**]

no pm [**15-min** | **24-hour**] { **ocn**} [**report** | **threshold**]

Syntax Description

15 min	Configures the 15 minute time interval for the PM parameters.
24-hour	Configures the 24 hour time interval for the PM parameters.
ocn	Displays the name of the layer.
report	Configures TCA reporting status of the controller.
threshold	Configures threshold on the controller.

Command Default

Enable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

The following example shows how to specify the 15 min PM interval for the OC controller and set threshold value for the layer:

```
RP/0/RP0:hostname(config)# controller ocn12 0/2/0/0
RP/0/RP0:hostname(config-ocn12)# pm 15-min ocn threshold cv-s 30
```

show controller (oc)

To display all the details of an OCn controller, use the **show controllers** command in the exec mode.

show controllers OC*n R/S/I/P*

Syntax Description

ocn	Displays the name of the ocn controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	read

Example

This example shows how to display the details of the oc192 controller:

```
RP/0/RP0:hostname # show controllers oc192 0/11/0/0
```

```
Tue Mar 17 23:57:59.773 UTC

Port OC192 0/11/0/0:

Status:
Primary State: Down

Sec admin State: Normal

Derived State: In Service

Loopback: None

SECTION
  LOF = 1          LOS    = 1                           BIP(B1) = 0
Overhead
J0 Transmit:    (0)
J0 Receive:     (0)
J0 Expected:    (0)

LINE
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B2) = 0
```

```
Last clearing of "show controllers SONET" counters never

Detected Alarms: SLOF
Masked Alarms: None
Detected Alerts: None
Masked Alerts: None

Framing: SONET
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6
  Clock source: internal (actual) line (configured)
```

Note Run *do show controller oc R/S/I/P* when command is executed in config mode.

threshold (oc)

To configure threshold for B1 BER threshold crossing alert (TCA) on an OCn controller, use the **threshold** command in the config mode. To delete the threshold for B1 BER TCA from an OCn controller, use the **no** form of this command.

threshold [**b1-tca** *value*]

no threshold [**b1-tca** | **b2-tca** | **sf-ber** | **sd-ber** *value*]

Syntax Description

b1-tca	Configures B1 BER threshold for the threshold crossing alert (tca) on the OCn controller.
	Name of the controller. Following are the valid value of n: • OC48 • OC192
value	Configures the bit error rate value. The valid range of bit error rate is from 3 to 9. The default value is 6.

Command Default

TCA thresholds : B1=10e-6 B2=10e-6

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the threshold for B1 BER TCA on the OC48 controller:

```
RP/0/RP0:hostname(config)# controller oc48 0/0/0/1
RP/0/RP0:hostname(config-oc48)# threshold b1-tca 7
```

Controllers STSn Command Reference

This chapter describes the commands to configure the STSn controller.

controller (sts)

To configure an STSn controller, use the **controller** command in the config mode. To delete an STSn controller, use the **no** form of this command.

controller sts*n R/S/I/P*

no controller sts*n R/S/I/P*

Syntax Description

stsn	Configures an STSn controller. The range of n is from 48c to 192c.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

send : (2)

expected : (2)

receive : (2)

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to access the interface instance of an sts48c controller on port1:

```
RP/0/RP0:hostname(config)# controller sts-48c 0/0/0/1
```

overhead j1

To configure overhead value of an STSn controller, use the **overhead j1** command in the config mode. To delete the overhead value of an STSn controller, use the **no** form of this command.

overhead j1 {**send** | **expected**} [**16Bytes** | **64Bytes**] *value*

no overhead j1 {**expected**}

Syntax Description

send	Configures the transmitted trace identifier of the STSn controller.
expected	Configures the expected trace identifier of the STSn controller.
16Bytes	Configures the 16 bytes path trace for the STSn controller.
64Bytes	Configures the 64 bytes path trace for the STSn controller.
value	Enters the ASCII text for the STSn controller.

Command Default

2 stands 64 byte mode

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the overhead j1 value of the STS48c controller:

```
RP/0/RP0:hostname(config)# controller sts-48c 0/0/0/1
RP/0/RP0:hostname(config-sts48c)# overhead j1 expected 64Bytes abxc
```

pm (sts)

To configure the pm parameters of an STSn controller, use the **pm** command in the config mode. To delete the pm parameters of an STSn controller, use the **no** form of this command.

pm [**15-min** | **24-hour**] {**sts**} [**report** *status* | **threshold** *value*]

no pm [**15-min** | **24-hour**] {**sts**} [**report** *status* | **threshold** *value*]

Syntax Description

15 min	Configures the 15 minute time interval for the PM parameters.
24-hour	Configures the 24 hour time interval for the PM parameters.
sts	Displays the name of the layer.
report	Configures the TCA reporting status of the controller.
status	Configures the reporting status of the controller.
threshold	Configures threshold on the controller.
value	Configures the threshold value of the controller.

Command Default

Enable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

The following example shows how to specify the 15 min PM interval for the STS controller and set threshold value for the layer:

```
RP/0/RP0:hostname(config)# controller sts-48c 0/0/0/1
RP/0/RP0:hostname(config-sts48c)# pm 15-min sts threshold cv-p 30
```

show controllers (sts)

To display all the details of an STSn controller, use the **show controllers** command in the exec mode.

show controllers sts*n R/S/I/P*

Syntax Description

stsn	Displays the name of the STSn controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	read

Example

This example shows how to display the details of an STS48c controller:

```
RP/0/RP0:hostname # show controllers sts48c 0/0/0/1
```

```
  Primary State: Down

Sec Admin State: Normal

Derived State: In Service

PATH
  FEBE   = 0          BIP(B3) = 0
  NEWPTR = 0          PSE    = 0          NSE  = 0
Detected Alarms:       None

Mask for Detected->Asserted:      None

Detected Alerts: None
Mask for Detected->Reported: None
Payload Scrambling: Disabled
C2 State: Stable   C2_rx = 0x0 (0)   C2_tx = 0x0 (0) / Scrambling Derived
B3 = 10e-6
Overhead J1
Transmit        : (2)
Received        : (2)
Expected        : (2)
```

```
 performace_monitoring enabled
============================================================
```

Note Run *do show controller stsn R/S/I/P* when command is executed in config mode.

threshold

To configure threshold for B3 bit error rate (BER) threshold crossing alert (TCA) on an STSn controller, use the **threshold** command in the config mode. To delete the threshold for B3 BER TCA from an STSn controller, use the **no** form of this command.

threshold [**b3-tca** *value*]

no threshold [**b3-tca** *value*]

Syntax Description

b3-tca	Configures the B3 BER threshold for the TCA on the STSn controller.
value	Configures the BER value. The valid range of BER is from 3 to 9. The default value is 6.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the threshold for B3 BER TCA on the STS48c controller:

```
RP/0/RP0:hostname(config)# controller sts-48c 0/0/0/1
RP/0/RP0:hostname(config-sts48c)# threshold b3-tca 7
```

Controllers STMn Command Reference

This chapter describes the commands to configure the STMn controller.

controller (stm)

To configure a STMn controller, use the **controller** command in the config mode. To delete a STMn controller, use the **no** form of this command.

controller stm*n R/S/I/P*

no controller stm*n R/S/I/P*

Syntax Description

stmn	Configures an STMn controller. The range of n is 1, 4, 16, 64, 256.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

send : (0)

expected : (0)

receive : (0)

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to access the interface instance of a stm64 controller on port2:

```
RP/0/RP0:hostname(config)# controller stm64 0/0/0/2
```

overhead j0

To configure overhead value on an STMn controller, use the **overhead j0** command in the config mode. To delete the overhead value from a STMn controller, use the **no** form of this command.

overhead j0 [**expected** | **send** [**1Byte** | **16Bytes**]

no overhead j0 {**length**} [**1Byte** | **16Bytes**] [**send** | **expected**] *value*

Syntax Description

1Byte	Configures the 1 byte path trace for the STMn controller.
16Bytes	Configures the 16 bytes path trace for the STMn controller.
send	Configures the transmitted trace identifier of the STMn controller.
expected	Configures the expected trace identifier of the STMn controller.
value	Enters the ASCII text for the STMn controller.

Command Default

0 stand byte mode

BER thresholds: SF=10e-3 SD=10e-6

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the overhead j0 value on the stm64 controller:

```
RP/0/RP0:hostname(config)# controller stm64 0/0/0/2
RP/0/RP0:hostname(config-stm64)# overhead j0 length 1Byte expected 45
```

pm stm

To configure the pm parameters of an STM controller, use the **pm** command in the config mode. To delete the pm parameters of an STM controller, use the **no** form of this command.

pm [**15-min** | **24-hour**] {**stm**} [**report** *status* | **threshold** *value*]

no pm [**15-min** | **24-hour**] {**stm**} [**report** *status* | **threshold** *value*]

Syntax Description

15 min	Configures the 15 minute time interval for the PM parameters.
24-hour	Configures the 24 hour time interval for the PM parameters.
stm	Displays the name of the layer.
report	Configures the TCA reporting status of the controller.
report status	Configures the reporting status of the controller.
threshold	Configures threshold on the controller.
threshold value	Configures the threshold value on the controller.

Command Default

Enable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

The following example shows how to specify the 15 min PM interval for the stm controller and set threshold value for the layer:

```
RP/0/RP0:hostname(config)# controller stm4 0/2/0/0
RP/0/RP0:hostname(config-stm4)# pm 15-min stm threshold eb-l-ne 30
```

show controllers (stm)

To display all the details of an STMn controller, use the **show controllers** command in the exec mode.

show controllers stm*n R/S/I/P*

Syntax Description

stmn	Displays the name of the STMn controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	read

Example

This example shows how to display the details of the stm64 controller:

```
RP/0/RP0:hostname # show controllers stm64 0/2/0/10
```

```
Port STM640/2/0/10:

Status:
 Primary State: Down

Sec admin State: Normal

Derived State: In Service

Loopback: None

REGENERATOR SECTION
  LOF = 0          LOS    = 1                            RS-BIP  = 0
Overhead
J0 Transmit:    (2)
J0 Receive:     (2)
J0 Expected:    (2)

MULTIPLEX SECTION
  AIS = 0          RDI    = 0          FEBE = 0          MS-BIP  = 0

Last clearing of "show controllers SDH" counters never
```

```
Detected Alarms: LOS
Masked Alarms: None
Detected Alerts: None
Masked Alerts: None

Framing: SONET
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6
  Clock source: internal (actual) line (configured)
```

Note Run *do show controller stmn R/S/I/P* when command is executed in config mode.

threshold

To configure threshold for B3 bit error rate (BER) threshold crossing alert (TCA) on a STMn controller, use the **threshold** command in the config mode. To delete the threshold for B3 BER TCA from a STMn controller, use the **no** form of this command.

threshold {**b1-tca** | **b2-tca** | **sd-ber** | **sf-ber**} *value*

no threshold {**b1-tca** | **b2-tca** | **sd-ber** | **sf-ber**} *value*

Syntax Description

b1-tca	Configures the B1 BER threshold for the TCA on the STMn controller.
b2-tca	Configures the B2 BER threshold for the TCA on the STMn controller.
sd-ber	Configures the signal degrade BER threshold on the STMn controller.
sf-ber	Configures the signal fail BER threshold on the STMn controller.
value	Configures the BER value. The BER value ranges from 3 to 9 and default value is 6 for b1-tca and b2-tca. For sd-ber it ranges from 5 to 9 and default value is 6. BER value for sf-ber ranges from 3 to 5 and default value is 3.

Command Default

TCA threshold : B1=10e-6 B2=10e-6

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the threshold for B3 BER TCA on the stm64 controller:

```
RP/0/RP0:hostname(config)# controller stm64 0/0/0/2
RP/0/RP0:hostname(config-stm64)# threshold b2-tca 7
```

Controllers VCn Command Reference

This chapter describes the commands to configure the VCn controller.

controller (vc)

To configure a VCn controller, use the **controller** command in the config mode. To delete a VCn controller, use the **no** form of this command.

controller vc*n R/S/I/P*

no controller vc*n R/S/I/P*

Syntax Description

vcn	Configures a VCn controller. The range of n is 4-16c, 4-64c.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

send: (2)

expected: (2)

receive: (2)

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to access the interface instance of a vc4-64c controller on port10:

```
RP/0/RP0:hostname(config)# controller vc4-64c 0/0/0/10
```

overhead j1

To configure overhead value on a VCn controller, use the **overhead j1** command in the config mode. To delete the overhead value from a VCn controller, use the **no** form of this command.

overhead j1 {**send** | **expected**} [**16Bytes** | **64Bytes**] *value*

no overhead j1 {**send** | **expected**} [**16Bytes** | **64Bytes**] *value*

Syntax Description

send	Configures the transmitted trace identifier of the VCn controller.
expected	Configures the expected trace identifier of the VCn controller.
16 Bytes	Configures the 16 bytes path trace for the VCn controller.
64 Bytes	Configures the 64 bytes path trace for the VCn controller.
value	Enters the ASCII text for the VCn controller.

Command Default

2 stands 64 byte mode

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the overhead j1 value on the vc4-64c controller:

```
RP/0/RP0:hostname(config)# controller vc4-64c 0/0/0/10
RP/0/RP0:hostname(config-vc4-64c)# overhead j1 send 64Bytes abc
```

pm (vc)

To configure the pm parameters of an VCn controller, use the **pm** command in the config mode. To delete the pm parameters of an VCn controller, use the **no** form of this command.

pm [**15-min** | **24-hour**] {**vc**} [**report** *status* | **threshold** *value*]

no pm [**15-min** | **24-hour**] {**vc**} [**report** *status* | **threshold** *value*]

Syntax Description

15 min	Configures the 15 minute time interval for the PM parameters.
24-hour	Configures the 24 hour time interval for the PM parameters.
vc	Displays the name of the layer.
report	Configures the TCA reporting status of the controller.
reporting status	Configures the reporting status of the controller.
threshold	Configures threshold on the controller.
threshold value	Configures the threshold value on the controller.

Command Default

Enable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

The following example shows how to specify the 15 min PM interval for the VC controller and set threshold value for the layer:

```
RP/0/RP0:hostname(config)# controller vc4-64c 0/0/0/10
RP/0/RP0:hostname(config-vc4-64c)# pm 15-min ho-vc threshold eb-p 20
```

show controllers

To display all the details of an VCn controller, use the **show controllers** command in the exec or config mode.

show controllers VC*n R/S/I/P*

Syntax Description

vcn	Displays the name of the VCn controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	read

Example

This example shows how to display the details of the vc4-16c controller:

```
RP/0/RP0:hostname # show controllers vc4-16c 0/0/0/8
```

```
PATH
  FEBE   = 6000       BIP(B3) = 6000
  NEWPTR = 0          PSE    = 0          NSE  = 0
Detected Alarms: AU-LOP AU-AIS HP-RDI HP-TIM HP-PLM HP-UNEQ

Mask for Detected->Asserted:AU-LOP AU-AIS HP-RDI HP-TIM HP-PLM HP-UNEQ

Detected Alerts:B3-TCA
Mask for Detected->Reported: None
Payload Scrambling: Disabled
C2 State: Unstable   C2_rx = 0x0 (0)   C2_tx = 0x0 (0) / Scrambling Derived
B3 = 10e-6
Overhead J1
Transmit             : (0)
Received             : (0)
Expected             : (16)
```

Note Run *do show controller vcn R/S/I/P* when command is executed in config mode.

threshold

To configure threshold for B3 bit error rate (BER) threshold crossing alert (TCA) on a VCn controller, use the **threshold** command in the config mode. To delete the threshold for B3 BER TCA from a VCn controller, use the **no** form of this command.

threshold [**b3-tca** *value*]

no threshold [**b3-tca** *value*]

Syntax Description

b3-tca	Configures B3 BER threshold for the TCA on the VCn controller.
value	Configures the BER value. The valid range of BER is from 3 to 9. The default value is 6.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sonet-sdh	write

Example

This example shows how to configure the threshold for B3 BER TCA on the vc4-64c controller:

```
RP/0/RP0:hostname(config)# controller vc4-64c 0/0/0/10
RP/0/RP0:hostname(config-vc4-64c)# threshold b3-tca 7
```

ODU Controller Command Reference

This chapter describes the commands to configure the ODUk controller.

controller oduk

To configure an ODUk controller, use the **controller oduk** command in the config mode. To delete the controller oduk, use the **no** form of this command.

controller oduk *R/S/I/P*
oduj [**tpn** *value*] [**ts** *value*]
no oduj [**tpn** *value*]

Syntax Description

oduk	Name of the controller. The valid range of k is from 0 to 4 (0, 1, 2, 1e , 2e, 3, 3-1, 3-2, 4 ,0, 1, 2e, 3, 3-1, 3-2).
oduj	Name of the controller. The valid range of j is from 0 to 4 (0, 1, 2, 1e , 2e, 3, 3-1, 3-2, 4 ,0, 1, 2e, 3, 3-1, 3-2).
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
tpn	TPN value ranges from 1 to 80. Tributary port number as allowed in G.70
value	Displays the tpn value.
ts	tributary slot string separated by (:) or (-) from 1 to no of ts \ in parent controller. (:) indicates individual tributary slot and (-) represent range.
value	Displays the ts value.

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before configuring the parameters of an ODUk controller, ensure that the ODUk controller is created.

Task ID

Task ID	Operation
otn	write

This example shows how to access an interface instance of an ODU1 controller on port 1.

```
RP/0/RP0:hostname (config)# controller odu1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# odu0 tpn 1 ts 1
```

gcc1

To configure general communication channel (GCC) on an ODUk controller, use the **gcc1** command in the config mode. To delete the gcc1, use the **no** form of this command.

gcc1
no gcc1

Command Default

Disable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure GCC on the ODU1 controller.

```
RP/0/RP0:hostname (config)# controller odu1 0/0/0/2
RP/0/RP0:hostname (config-odu1)# gcc1
```

loopback

To configure loopback on an ODUk controller, use the **loopback** command in the config mode. To delete this feature, use the **no** form of this command.

loopback [**internal** | **line**]
no loopback [**internal** | **line**]

Syntax Description

internal	Configures a terminal loopback on an ODUk controller.
line	Configures a line loopback on an ODUk controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to configure a terminal loopback on the ODU1 controller.

```
RP/0/RP0:hostname (config)# controller ODU1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# loopback internal
```

The following example shows how to configure a line loopback on the ODU1 controller.

```
RP/0/RP0:hostname (config)# controller ODU1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# loopback line
```

secondary-admin-state

To configure the secondary administrative state of an ODUk controller, use the **secondary-admin-state** command in the config mode. To remove the secondary administrative state of an ODUk controller, use the **no** form of this command.

secondary-admin-state [**maintenance** | **normal**]
no secondary-admin-state [**maintenance** | **normal**]

Syntax Description

maintenance	Configures the administrative state indicating that the controller is under maintenance.
normal	Configures the administrative state indicating that the controller is normal.

Command Default

Normal

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The primary administrative state of an ODUk controller must be no shutdown if you want to configure a second administrative state of the controller. The secondary administrative state of ODUk controllers inherits from the corresponding optics controllers. You cannot modify the secondary administrative state of an ODUk controller if a loopback is already configured on it.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to configure the secondary administrative state of the ODU1 controller.

```
RP/0/RP0:hostname (config)# controller odu1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# secondary-admin-state normal
```

show card state

To display a card state, use the **show platform** command in the exec or administration exec mode.

show platform

Command Modes

Exec mode

Administration Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sysmgr	read
root-lr	read

The following example shows how to display the card state in IOS XR mode:

```
RP/0/RP0:hostname# show platform
```

```
Wed Apr 15 21:28:10.626 UTC
Node name      Node type        Node state    Admin state   Config state
-----------------------------------------------------------------------------
0/0          NCS4K-24LR-O-S     OPERATIONAL      UP           NSHUT
0/1          NCS4K-20T-O-S      OPERATIONAL      UP           NSHUT
0/RP0        NCS4K-RP           OPERATIONAL      UP           NSHUT
0/RP1        NCS4K-RP           OPERATIONAL      UP           NSHUT
0/FC0        NCS4016-FC-M       OPERATIONAL      UP           NSHUT
0/FC1        NCS4016-FC-M       OPERATIONAL      UP           NSHUT
0/FC2        NCS4016-FC-M       OPERATIONAL      UP           NSHUT
0/FC3        NCS4016-FC-M       OPERATIONAL      UP           NSHUT
0/FT0        NCS4K-FTA          OPERATIONAL      UP           NSHUT
0/FT1        NCS4K-FTA          OPERATIONAL      UP           NSHUT
0/EC0        NCS4K-ECU          OPERATIONAL      UP           NSHUT
```

The following example shows how to display the card state in system admin mode:

```
sysadmin-vm: 0_RP1 # show platform
```

```
Wed Apr  15 21:27:40.651 UTC
Location  Card Type                HW State      SW State      Config State
-------------------------------------------------------------------------
0/1       NCS4K-20T-O-S            OPERATIONAL   N/A           NSHUT
0/RP0     NCS4K-RP                 OPERATIONAL   OPERATIONAL   NSHUT
```

```
0/RP1     NCS4K-RP                OPERATIONAL   OPERATIONAL   NSHUT
0/FC0     NCS4016-FC-M            OPERATIONAL   N/A           NSHUT
0/FC2     NCS4016-FC-M            OPERATIONAL   N/A           NSHUT
0/FC3     NCS4016-FC-M            OPERATIONAL   N/A           NSHUT
0/FT0     NCS4K-FTA               OPERATIONAL   N/A           NSHUT
0/FT1     NCS4K-FTA               OPERATIONAL   N/A           NSHUT
0/EC0     NCS4K-ECU               OPERATIONAL   N/A           NSHUT
```

show controllers

To display all the details of an ODUk/OTUk controller, use the **show controllers** command in the exec mode.

show controllers oduk/otuk *R/S/I/P* [**te** | **xc** | **odtu-details** | **prbs-details**]

Syntax Description

oduk/otuk	Displays the name of the ODUk/OTUk controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
te	Displays all the transport engineering details of the ODUk/OTU controller.
xc	Displays all the cross connection information of the ODUk/OTU controller.
odtu-details	Displays all the odtu information of the ODUk/OTU controller.
prbs-details	Displays all the prbs information of the ODUk/OTU controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

This example shows how to display the proactive protection details of the ODU1 controller:

```
RP/0/RP0:hostname # show controllers odu1 0/3/0/12
```

```
Wed Aug 13 12:29:40.652 IST

Port                                               : ODU1 0/3/0/12
Controller State                                   : Up
Secondary state                                    : Normal
Derived State                                      : In Service
Loopback mode                                      : None
```

```
BER Thresholds                                    : SF = 1.0E-3  SD = 1.0E-6

Performance Monitoring                            : Disable

Alarm Information:
AIS = 0 IAE = 0 BIAE = 0
SF_BER = 0      SD_BER = 0      BDI = 0
OCI = 0 LCK = 0 PTIM = 0
TIM = 0 CSF = 0 GFP LFD = 0
GFP LOCS = 0    GFP LOCCS = 0   GFP UPM = 0

Detected Alarms                                   : None

ODU TTI Sent

ODU TTI Received

ODU TTI Expected

Owner                                             : All
Resource State                                    : ODU Cross Connection
RP/0/0/CPU0:ios(config)#
```

```
RP/0/RP0:hostname # show controllers odu1 0/0/0/1 te
```

```
Thu Jul 31 15:05:39.954 IST

LOCAL_INFO

        router_id                                 :0.0.0.0
        ifindex                                   : 0
REMOTE_INFO

        router_id                                 :0.0.0.0
        ifindex                                   : 0

GMPLS TTI MODE  : Not Set
GMPLS TCM ID    : 0
```

```
RP/0/RP0:hostname # show controllers odu1 0/0/0/1 xc
```

```
Thu Jul 31 15:06:30.752 IST
Xconnect ID                                       : 0
FWD ref                                           :
FWD ref ifhandle                                  : 0

Owner                                             : All
Resource State                                    : ODU Open Connection
Xconnect status                                   : XCONNECT_NOT_SET
Xconnect Add RequestGMPLS Request Context Data
     Request Time                                 :
     Context Type                                 : NONE
     RM Type                                      : NONE
     Tunnel Info Type                             : NONE
Xconnect Delete RequestGMPLS Request Context Data
     Request Time                                 :
     Context Type                                 : NONE
     RM Type                                      : NONE
     Tunnel Info Type                             : NONE
```

```
RP/0/RP0:hostname # show controllers odu1 0/0/0/1 odtu-details
```

```
Mon Oct 12 15:58:20.812 IST

Port                                          : ODU1 0/0/0/0
ODU TS Granularity                            : 1.25G

Number Of Tributary Slots                     : 1-2
Used Tributary Slot                           : 1
Payload Type                                  : 20 (ODU multiplex structure
supporting ODTUjk)

TPN Value                                     : 0
Allocated Tributary Slot                      : 1
Allocated Parent Tributary Slot               :

Tributary Slots Allocation
_____________________________________________________________
Tributary Slots          Name            TPN
1               ODU00_0_0_0_10          1
```

show hw-module fpd

To display field-programmable device (FPD) compatibility for all modules or a specific module, use the **show hw-module fpd** command in the exec or administration exec mode.

show hw-module fpd {**location**} [*node-id* | *all*]

Syntax Description

location	Specifies the location of the module.
Node-ID	Specifies the node-id of the module. The node-id argument is expressed in the rack/slot/module notation.
all	Specifies the all nodes of the module. Use the all keyword to indicate all nodes.

Command Modes

Exec mode

Administration Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sysmgr	read
root-lr	read

The following example shows how to display FPD compatibility for all modules in the router:

```
RP/0/RP0:hostname# show hw-module fpd location all
```

```
Wed Apr 15 21:29:40.934 UTC
                                                FPD Versions
                                               =================
Location   Card type    HWver  FPD device   ATR Status   Running  Programd
-------------------------------------------------------------------------
0/1      NCS4K-20T-O-S   0.1    ZYNQ         CURRENT      1.51     1.51
0/1      NCS4K-20T-O-S   0.1    GENNUM       CURRENT      3.01     3.01
0/1      NCS4K-20T-O-S   0.1    DIGI2        CURRENT      2.03     2.03
0/1      NCS4K-20T-O-S   0.1    DIGI1        CURRENT      2.03     2.03
0/6      NCS4K-24LR-O-S  0.1    ZYNQ         NEED UPGD    4.04     4.04
0/7      NCS4K-24LR-O-S  0.1    ZYNQ         NEED UPGD    4.04     4.04
```

The following example shows how to display FPD compatibility for a specific module in the router:

```
RP/0/RP0:hostname# show hw-module location 0/0 fpd
```

```
Mon Jan 19 02:23:40.752 UTC
                                                FPD Versions
                                               =================
Location   Card type    HWver  FPD device   ATR Status  Running Programd
-----------------------------------------------------------------------------
0/0      NCS4K-20T-O-S   N/A   Backup-ZYNQ   NOT READY   N/A     N/A
0/0      NCS4K-20T-O-S   N/A   DIGI1         NOT READY   N/A     N/A
0/0      NCS4K-20T-O-S   N/A   DIGI2         NOT READY   N/A     N/A
0/0      NCS4K-20T-O-S   N/A   GENNUM        NOT READY   N/A     N/A
0/0      NCS4K-20T-O-S   N/A   Primary-ZYNQ  NOT READY   N/A     N/A
```

shutdown

To disable the configuration of ODUk/OTUk controller, use the **shutdown** command in the config mode. To delete the shutdown, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

Down

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to disable the configuration of the ODU/OTU1 controller:

```
RP/0/RP0:hostname (config)# controller odu1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# shutdown
```

tcm

To configure tandem connection monitoring (TCM) on an ODUk controller, use the **tcm** command in the config mode. To delete the TCM of the ODUk controller, use the **no** form of this command.

tcm {**id** *value*} {**permon-enable** | **threshold** [**pm-tca** | **sd** | **sf**] *value* | **tti** [**expected** | **send**] [**ascii** | **dapi** | **hex** | **operator-specific** | **sapi**] *string* }

Syntax Description

id	Configures the TCM ID on an ODUk controller.
value	Configures the tandem connection monitoring ID value. The valid range of TCM ID is from 1 to 6.
permon enable	Enables the performance monitoring on an ODUk controller.
threshold	Configures threshold for signal failure and signal degrade.
pm-tca	Configures threshold crossing alert (TCA) on an ODUk controller.
value	Configures the threshold crossing alert value. The valid range is from 3 to 9 and default value is 3.
sd	Configures signal degrade (SD) threshold on an ODUk controller.
value	Configures the signal degrade threshold value. The valid range is from 3 to 9 and default value is 6.
sf	Configures signal failure (SF) threshold on an ODUk controller.
value	Configures the signal failure threshold value. The valid range is from 1 to 9 and default value is 3.
tti	Configures the trail trace identifier (TTI) on an ODUk controller.
expected	Configures the expected TTI of the ODUk controller.
send	Configures the transmitted TTI of the ODUk controller.
ascii	Configures the ASCII string of the TTI.
dapi	Configures the destination access point identifier of the TTI.
hex	Configures the hexadecimal string of the TTI.
operator-specific	Configures the operator specific string of the TTI.
sapi	Configures the source access point identifier of the TTI.

string	Configures a hexadecimal string that must be an even number and a maximum of 64 characters is allowed in this string.

Command Default

Disable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before configuring TCM on an ODUk controller, ensure that the ODUk controller is created.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the TCM ID on an ODU1 controller:

```
RP/0/RP0:hostname(config)# controller odu1 0/0/0/1
RP/0/RP0:hostname(config-odu1)# tcm id 3
```

threshold

To configure threshold for signal failure and signal degrade on an ODUk controller and tcm, use the **threshold** command in the config mode. To delete the threshold, use the **no** form of this command.

threshold [**sf** *value*]
no threshold [**sf** *value*]

threshold sd *value*
no threshold sd *value*

Syntax Description

sf	Configures threshold for the signal failure on the ODUk controller.
value	Signal failure threshold. The valid range of signal failure is from 1 to 9. The default value is 3.
sd	Configures threshold for the signal degrade on the ODUk controller.
value	Signal degrade threshold. The valid range of signal degrade is from 3 to 9. The default value is 6.

Command Default

By default, threshold for signal failure is 3 and signal degrade is 6 for a given ODUk controller.

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to configure threshold for signal failure and signal degrade on the ODU1 controller:

```
RP/0/RP0:hostname (config)# controller odu1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# threshold sf 4
RP/0/RP0:hostname (config-odu1)# threshold sd 6
```

Example

The following example shows how to configure threshold for signal failure and signal degrade on the TCM3 of ODU1 controller:

```
RP/0/RP0:hostname (config)# controller odu1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# tcm id 3
RP/0/RP0:hostname (config-odu1-tcm3)# threshold sf 5
RP/0/RP0:hostname (config-odu1-tcm3)# threshold sd 7
```

tsg

To configure tributary slot granularity (TSG) level on an ODUk controller, use the **tsg** command in the config mode. To delete the tsg, use the **no** form of this command.

tsg *value*
no tsg *value*

Syntax Description

tsg	Configures the TSG level on an ODU controller. **Note** You need to commit tsg configuration, and shut commands separately.
value	Tributary slot granularity. The default value is 1.25G and it can be changed to 2.5G.

Command Default

By default, TSG level is 1.25G on a given ODUk controller.

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can configure TSG on an ODUk controller only if the system is in the shut mode. The default value for TSG is 1.25G and it can be changed to 2.5G for ODU1, ODU2 , ODU3 and ODU4 controllers only.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to configure tsg on an ODU1 controller:

```
RP/0/RP0:hostname (config)# controller odu1 0/0/0/1
RP/0/RP0:hostname (config-odu1)# tsg 1.25G

RP/0/RP0:hostname (config-odu1)# shut
```

tti

To configure trail trace identifier (TTI) of an ODUk controller, use the **tti** command in the config mode. To delete the TTI of the ODUk controller, use the **no** form of this command.

tti {**expected** | **send**} [**ascii** | **dapi** | **hex** | **operator-specific** | **sapi**] *value*
no tti {**expected** | **send**} [**ascii** | **dapi** | **hex** | **operator-specific** | **sapi**] *value*

Syntax Description

expected	Configures the expected TTI of the ODUk controller.
send	Configures the transmitted TTI of the ODUk controller.
ascii	Configures the ASCII string of the TTI.
dapi	Configures the destination access point identifier of the TTI.
hex	Configures the hexadecimal string of the TTI.
operator-specific	Configures the operator specific string of the TTI.
sapi	Configures the source access point identifier of the TTI.
string	Configures a hexadecimal string that must be an even number and a maximum of 64 characters is allowed in this string.

Command Default

By default, TTI value is 0 for an ODUk controller.

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before configuring the TTI on an ODUk controller, ensure that the ODUk controller is created.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the send TTI of the ODU1 controller in hexadecimal format:

```
RP/0/RP0:hostname(config)# controller odu1 0/0/0/1
RP/0/RP0:hostname(config-odu1)# tti sent hex abcd
```

This example shows how to configure the expected TTI on the TCM3 of the ODU1 controller in ascii format:

```
RP/0/RP0:hostname(config)# controller odu1 0/0/0/1
RP/0/RP0:hostname(config-odu1)# tcm id 3
RP/0/RP0:hostname(config-odu1)# tti expected ascii abc
```

upgrade hw-module fpd

To manually upgrade the current field-programmable device (FPD) image package on a module, use the **upgrade hw-module fpd** command in administration exec mode.

upgrade hw-module {**location**} [*node-id* | **all**] {**fpd**} {**all** | **Primary-ZYNQ** | **Backup-ZYNQ**}

Syntax Description

location	Specifies the location to upgrade the FPD image.
Node-ID	Specifies the node-id to upgrade the FPD image. The node-id argument is expressed in the rack/slot/module notation.
all	Specifies all the nodes to upgrade the FPD image.
all	Upgrades all the FPD images on the selected module.
Primary-ZYNQ	Upgrades Primary-ZYNQ FPD image on the selected module.
Backup-ZYNQ	Upgrades Backup-ZYNQ FPD image on the selected module.

Command Default

None

Command Modes

Administration Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note The use of the force option when doing a fpd upgrade is not recommended except under explicit direction from Cisco engineering or TAC.

During the upgrade procedure, the module must be offline (shut down but powered).

Task ID

Task ID	Operation
system	read, write
sysmgr	read, write

The following example shows how to upgrade all the FPD's on all the locations:

```
RP/0/RP0:hostname# admin
RP/0/RP0:hostname(admin)# upgrade hw-module location all fpd all
```

The following example shows how to upgrade the Primary-ZYNQ FPD's on a specific location:

```
RP/0/RP0:hostname# admin
RP/0/RP0:hostname(admin)# upgrade hw-module location 0/1 fpd Primary-ZYNQ
```

OTU Controller Command Reference

This chapter describes commands to configure the OTUk controllers.

controller otuk

To configure an OTUk controller, use the **controller** command in the global configuration mode.

controller otuk *Rack/Slot/Instance/Port*

Syntax Description

otuk	Name of the controller. The valid range of k is from 1 to 4.
Rack/Slot/Instance/Port	Interface instance of the controller.

Command Modes

Global configuration (config)

Command History

Release	Modification
5.2.1	This command was introduced.

Usage Guidelines

Before configuring the parameters of an OTUk controller, ensure that the OTUk controller is created.

Example

The following example shows how to access an interface instance of an OTU1 controller on port 1.

```
Router(config)# controller OTU1 0/0/0/1
```

fec

To configure the forward error connection (FEC) on an OTUk controller, use the **fec** command in the OTUk controller configuration mode.

fec [**EnhancedHG20** | **EnhancedI4** | **EnhancedI7** | **EnhancedSwizzle** | **Standard**]

Syntax Description

EnhancedHG20	Configures high-gain enhanced FEC with 7 percent OTN overhead.
EnhancedI4	Configures G.975.1.4 enhanced FEC with 7 percent OTN overhead.
EnhancedI7	Configures G.975.1.7 enhanced FEC with 20 percent OTN overhead.
Enhancedwizzle	Configures swizzle FEC with 6.7 percent OTN overhead.
Standard	Configures Standard G.975 Reed-Salomon algorithm with 7 percent overhead.

Command Default

By default, standard FEC is enabled.

Command Modes

OTUk controller configuration (config-otuk)

Command History

Release	Modification
5.2.1	This command was introduced.

Usage Guidelines

You can configure FEC for an OTUk controller only if the system is in the shut mode. For the OTU1 controller, you can configure only standard G.975 FEC. For the OTU2 controller, you can configure standard G.975 FEC, G.975.1.4 enhanced FEC, and G.975.1.7 enhanced FEC.

Example

The following example shows how to configure standard G.975 FEC on the OTU1 controller.

```
Router(config)# controller OTU1 0/0/0/1
Router(config-otu1)# fec Standard
```

gcc0

To configure general communication channel (GCC) on an OTUk controller, use the **gcc0** command in the OTUk controller configuration mode.

gcc0

Command Default By default, GCC is disabled.

Command Modes OTUk controller configuration (config-otuk)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to configure GCC on the OTU1 controller.

```
Router(config)# controller OTU1 0/0/0/1
Router(config-otu1)# gcc0
```

loopback

To configure loopback on an OTUk controller, use the **loopback** command in the OTUk controller configuration mode.

loopback [**internal** | **line**]

Syntax Description

internal	Configures a terminal loopback on an OTUk controller.
line	Configures a line loopback on an OTUk controller.

Command Default

By default, loopback is disabled.

Command Modes

OTUk controller configuration (config-otuk)

Command History

Release	Modification
5.2.1	This command was introduced.

Usage Guidelines

You can configure loopback on an OTUk controller only if the secondary administrative state of the controller is maintenance.

Example

The following example shows how to configure a terminal loopback on the OTU1 controller.

```
Router(config)# controller OTU1 0/0/0/1
Router(config-otu1)# loopback internal
```

secondary-admin-state

To configure the secondary administrative state of an OTUK controller, use the **secondary-admin-state** command in the OTUk controller configuration mode.

secondary-admin-state [**automatic-in-service** | **maintenance** | **normal**]

Syntax Description

automatic-in-service	Configures the administrative state indicating that the controller is in service.
maintenance	Configures the administrative state indicating that the controller is under maintenance.
normal	Configures the administrative state indicating that the controller is normal.

Command Default

By default, the secondary administrative state of an OTUk controller is normal.

Command Modes

OTUk controller configuration (config-otuk)

Command History

Release	Modification
5.2.1	This command was introduced.

Usage Guidelines

The primary administrative state of an OTUk controller must be no shutdown if you want to configure a second administrative state of the controller. The secondary administrative state of OTUk controllers is inherited by the corresponding optics controllers. You cannot modify the secondary administrative state of an OTUk controller if a loopback is already configured on it.

Example

The following example shows how to configure the secondary administrative state as in service of the OTU1 controller.

```
Router(config)# controller OTU1 0/0/0/1
Router(config-otu1)# secondary-admin-state automatic-in-service
```

threshold

To configure threshold for signal failure and signal degrade on an OTUk controller, use the **threshold** command in the OTUk controller configuration mode.

threshold sf *value*

threshold sd *value*

Syntax Description

sf	Configures threshold for the signal failure on the OTUk controller.
value	Signal failure threshold. The valid range of signal failure is from 1 to 9. The default value is 3.
sd	Configures threshold for the signal degrade on the OTUk controller.
value	Signal degrade threshold. The valid range of signal failure is from 3 to 9. The default value is 6.

Command Default

By default, threshold for signal failure is 3 and signal degrade is 6 for a given OTUk controller.

Command Modes

OTUk controller configuration (config-otuk)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to configure threshold for signal failure and signal degrade on the OTU1 controller.

```
Router(config)# controller OTU1 0/0/0/1
Router(config-otu1)# threshold sf 5
Router(config-otu1)# threshold sd 5
```

tti

To configure trail trace identifier (TTI) of the OTUk controller, use the **tti** command in the OTUk controller configuration mode.

tti expected [**ascii** *text* | **hex** *text*]

tti send [**ascii** *text* | **hex** *text*]

Syntax Description

expected	Configures the expected TTI of the OTUk controller.
send	Configures the transmitted TTI of the OTUk controller.
ascii	Configures the ASCII string of the TTI.
text	ASCII text. A maximum of 32 characters is allowed in the ASCII string.
hex	Configures the hexadecimal string of the TTI.
text	Hexadecimal text. A hexadecimal string must be an even number and a maximum of 64 characters is allowed in this string.

Command Modes

OTUk controller configuration (config-otuk)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to configure the TTI of the OTU1 controller.

```
Router(config)# controller OTU1 0/0/0/1
Router(config-otu1)# tti expected ascii abc
Router(config-otu1)# tti expected hex ascx
Router(config-otu1)# tti send ascii zzz
Router(config-otu1)# tti send hex abcd
```

srlg

To configure shared risk link groups (SRLGs) for an OTUk controller, use the **srlg** command in the OTUk controller configuration mode.

srlg [**set** *index values*]

Syntax Description

set	Configures a set of SRLGs.
index	Configures the index of the given SRLG set. The valid range of index is from 1 to 17.
values	Configures the value of the network SRLG. The valid range of values is from 0 to 4294967294.

Command Modes

OTUk controller configuration (config-otuk)

Command History

Release	Modification
5.2.1	This command was introduced.

Usage Guidelines

You can create a maximum of 100 SRLGs distributed in 17 sets for a given OTUk controller. The first 16 sets can contain a maximum of six values and the seventeenth set can contain a maximum of four values.

Example

The following example shows how to configure a second set containing six SRLGs for the OTU1 controller.

```
Router(config)# controller OTU1 0/0/0/1
Router(config-otu1)# srlg set 2 3 4 5 6 7 9
```

interface gcc0

To enter the configuration mode of GCC interface on an OTUk controller, use the **interface gcc0** command in the global configuration mode.

interface gcc0 *Rack/Slot/Instance/Port*

Command Default

By default, GCC is disabled.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to enter the configuration mode of GCC interface on an OTU controller.

```
Router(config)# interface gcc0 0/0/0/0
```

show controllers

To display all the details of an OTUk controller, use the **show controller** command in the global configuration mode.

show controllers otuk *Rack/Slot/Instance/Port*

show controllers otuk *Rack/Slot/Instance/Port* **te**

show controllers otuk *Rack/Slot/Instance/Port* **proactive**

Syntax Description

otuk	Name of the OTUk controller.
Rack/Slot/Instance/Port	Interface instance of the OTUk controller.
te	Displays all the transport engineering details of the OTUk controller.
proctive	Displays all the proactive protection details of the OTUk controller.

Command Modes

Global configuration (config)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to display the proactive protection details of the OTU1 controller.

```
Router(config)# show controllers otu1 0/0/0/1 proactive
```

```
Proactive Protection Status               : OFF
Proactive Protection State                :In Active -Interface is Up
Inputs affecting proactive protection state:
        Secondary admin state             : Normal
        Trigger threshold                 : 0E-0       (Default 1E-4)
        Revert threshold                  : 0E-0       (Default 1E-4)
        Trigger integration window        : 0 ms
        Revert integration window         : 0 ms
        Received APS                      : NA
        Transmitted APS                   : NA
```

show interfaces gcc0

To display all the interfaces on which GCC is configured, use the **show interfaces gcc0** command in the global configuration mode.

show interfaces gcc0 *Rack/Slot/Instance/Port*

Syntax Description

Rack/Slot/Instance/Port	Interface instance of the OTUk controller.

Command Modes

Global configuration (config)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to display all the interfaces on which GCC is configured.

```
Router(config)# show interfaces gcc0 0/1/0/0
```

```
GCC00/1/0/0 is up, line protocol is up
  Interface state transitions: 2
  Hardware is GCC0
  Internet address is 1.1.1.1/24
  MTU 4474 bytes, BW 4294967295 Kbit (Max: 4294967295 Kbit)
     reliability Unknown, txload Unknown, rxload Unknown
  Encapsulation PPP,  loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP
  Last input Unknown, output Unknown
  Last clearing of "show interface" counters Unknown
  Input/output data rate is disabled
```

show ip interfaces br

To display IP address and status of all the interfaces, use the **show ip interfaces br** command in the privileged mode.

show ip interfaces *Rack/Slot/Instance/Port*
show ip interfaces br *Rack/Slot/Instance/Port*

Syntax Description

Rack/Slot/Instance/Port	Interface instance of the OTUk controller.
br	Br shows the brief details of all the interfaces .

Command Modes

Privileged (#)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to display IP address and brief status of all the interfaces.

```
Router # show ip interfaces br
```

```
Wed Jan  5 05:04:46.659 UTC
Interface                      IP-Address      Status                Protocol
GCC00/0/0/0                    1.1.1.1         Up                    Down
MgmtEth0/RP1/CPU0/0            unassigned      Shutdown              Down
```

Fabric Management Commands

This chapters provides details for the fabric management commands.

show asic-errors SFE

To display asic errors for the Switch Fabric Element (SFE), use the **show asic-errors SFE** command in the Administration EXEC mode.

show asic-errors SFE *element-id* **location** *location-id*

Syntax Description

element-id	SFE instance ID
location-id	Location ID of RP

Command Default

None

Command Modes

Administration EXEC

Command History

Release	Modification
Release 5.2.4	This command was first introduced.
Release 6.0.1	The **SFE** keyword was added.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sfe	read

Example

This example show how to use the **show asic-errors SFE** command:

```
sysadmin-vm:0_RP0# show asic-errors SFE 0 all location 0/RP0
Wed Apr  20 06:31:49.555 UTC
all location 0/RP0
************************************************************
*                          Instance:0                      *
************************************************************
************************************************************
*                    Single Bit Errors                     *
************************************************************
************************************************************
*                   Multiple Bit Errors                    *
************************************************************
************************************************************
*                      Parity Errors                       *
************************************************************
```

```
************************************************************
*                      Barrier Errors                      *
************************************************************
************************************************************
*                    Unexpected Errors                     *
************************************************************
************************************************************
*                       Link Errors                        *
************************************************************
NCS-4000, , 0/RP0, sfe[0]
Name            : RTP.General_Interrupt_Register.LinkIntegrityChangedInt
Leaf ID         : 0x20026029
Error count     : 1
Last clearing   : Tue Apr 19 19:03:45 2016
Last N errors   : 1
------------------------------------------------------------
First N errors.
@Time, Error-Data
----------------------------------------
Apr 19 19:03:45.595144:              Name  Address     Value
                    Link_Integrity_Vector 0x000001a8 0x0000000000000000000e070707000000
------------------------------------------------------------
NCS-4000, , 0/RP0, sfe[0]
Name            : RTP.General_Interrupt_Register.UnicastTableChangedInt
Leaf ID         : 0x2002602a
Error count     : 4
Last clearing   : Tue Apr 19 19:03:42 2016
Last N errors   : 4
```

show controller fabric plane

To display the details about the fabric plane, use the **show controller fabric plane** command in the Administration EXEC mode.

show controller fabric plane {**all** | **plane-id**} [**statistics**] [**brief | detail**]

Syntax Description

plane-id	Displays details of the selected plane number. Range is from 0 to 3.
all	Displays information about all the system fabric planes.
statistics	Displays plane statistics.
brief	Displays brief information about the system fabric plane or plane statistics.
detail	Displays detailed information about the system fabric plane or plane statistics.

Command Default

None

Command Modes

Administration EXEC mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.
Release 6.0.1	The display output has been modified to show the plane mode details.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sfe	read

Example

This example shows how to use the **show controller fabric plane** command:

```
sysadmin-vm:0_RP0# show controller fabric plane all


Plane Admin Plane  Plane  up->dn  up->mcast
Id    State State  Mode   counter   counter
-------------------------------------
0     UP    UP       SC          0         0
1     UP    UP       SC          0         0
```

```
2       UP      UP          SC              0           0
3       UP      UP          SC              0           0
```

Field	Description
Plane ID	Plane ID number.
Admin State	Admin status of the plane (up or down).
Plane State	Plane status (shut or unshut).
Plane Mode	Plane mode indicates single chassis or multi-chassis system.
up-dn counter	Plane counter.
up-mcast counter	Counter to indicate the if any of the links are down.

show controller sfe driver rack

To display the Switch Fabric Element (SFE) driver information, use the **show controller sfe driver rack** command in the Administration EXEC mode.

show controller sfe driver rack *rack-id*

Syntax Description

rack-id	The ID of the rack whose details need to be displayed.

Command Default

None

Command Modes

Administration EXEC

Command History

Release	Modification
Release 5.2.4	This command was first introduced.
Release 6.0.1	The output has been modified to show the Asic Class details.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sfe	read

Example

This example shows how to use the **show controller sfe driver rack** command:

```
sysadmin-vm:0_RP# show controller sfe driver rack 0
SFE Driver information
================================================================================

Driver Version: 1   (1.1)

Functional role: Active,   ISSU role: NA
Rack: 0/RP0, Type: lcc, Number: 0, IP Address: 192.0.44.1
Startup time       : 2016 Feb 11 13:58:55.646
Availability Masks :
     Card: 0xF       Asic: 0x1C71C7       Exp Asic: 0x1C71C7
Unicast/Multicast (ratio) : 0
+-------------------------------------------------------------+
|Process  | Connection | Registration| Connection | DLL          |
|/Lib     | status     | status      | requests   | registration |
+-------------------------------------------------------------+
| PM      |  Active    |  n/a        |           1|  n/a         |
| PL-LOCAL|  Active    |  Active     |           1|  n/a         |
```

```
| FSDB    |  Active    |  Active     |           1|  n/a         |
| FGID    |  Active    |  Active     |           1|  n/a         |
| CM      |  Active    |  Active     |           1|  n/a         |
| CCC     |  Active    |  n/a        |           1|  n/a         |
| GASPP   |  n/a       |  n/a        |         n/a|  No          |
| CIH     |  n/a       |  n/a        |         n/a|  Yes         |
+-------------------------------------------------------------+

Asics :
HP - HotPlug event,  PON - Power ON reset,     WB - Warm Boot,  A - All
HR - Hard Reset,     DC  - Disconnect signal,  DL - DownLoad
+-------------------------------------------------------------------------------------+
| Asic inst.|card|HP|Asic| Asic  | Admin|plane| Fgid| Asic State |DC| Last  |PON|HR |
|  (R/S/A)  |pwrd|  |type| class | /Oper|/grp | DL  |            |  | init  |(#)|(#)|
+-------------------------------------------------------------------------------------+
| 0/FC0/0   | UP | 1|s123|  FE3600| UP/UP| 0/A | DONE| NRML       | 0| PON   |  1|  0|
| 0/FC0/1   | UP | 1|s123|  FE3600| UP/UP| 0/A | DONE| NRML       | 0| PON   |  1|  0|
| 0/FC0/2   | UP | 1|s123|  FE3600| UP/UP| 0/A | DONE| NRML       | 0| PON   |  1|  0|
| 0/FC0/0   | UP | 1|s123|  FE1600| UP/UP| 0/A | DONE| NRML       | 0| PON   |  1|  0|
| 0/FC0/1   | UP | 1|s123|  FE1600| UP/UP| 0/A | DONE| NRML       | 0| PON   |  1|  0|
| 0/FC0/2   | UP | 1|s123|  FE1600| UP/UP| 0/A | DONE| NRML       | 0| PON   |  1|  0|
```

Field	Description
Process / Lib	External process name
Connection Status	State of SFE connection with external process(es)
Registration Status	State of SFE registration with external process(es)
Connection Requests	SFE connection request numbers with external process
DLL registration	DLL registration status
Asic inst. R/S/A	Asic instance number (Rack/ slot/ asic format)
Card PWRD	Card power status
HP	Hot plug attach status
Asic type	SFE mode - s13, s123, s2
Asic Class	SFE asic type - FE3600, FE1600
Admin/ Oper	Admin operation status from FSDB
Plane/ grp	Plane number
Fgid/ DL	FGID download status (Empty/ Done)
Asic State	Status of the ASIC
DC	Disconnect Status
Last init	Last Initialization Type - WB, PON, HPON
PON	Power or reset counters
HR	Hard reset counters

show controller sfe statistics

To display the Switch Fabric Element (SFE) statistics, use the **show controller sfe statistics** command in the Administration EXEC mode.

show controller sfe statistics asic-type [**FE3200** | **FE1600**] **block** *block-stats* **instance** { **asic-instance** | **all** } **location** { *node-id* | **all**}

Syntax Description

asic-type	Type of FE (FE1600 or 3200).
block *block-stats*	SFE block type. The possible options are: • CCS statistics - valid for FE1600 and FE3200 • DCH statistics - valid for FE1600 and FE3200 • DCL statistics - valid for FE1600 and FE3200 • DCM statistics - valid for FE3200 • DCMA statistics - valid for FE1600 • ECI statistics - valid for FE1600 • FMAC statistics - valid for FE1600 • FSRD statistics - valid for FE3200 • MESH statistics - valid for FE3200 • RTP statistics - valid for FE1600 and FE3200
instance	Indicates an instance.
asic-instance	Displays statistics for a specific ASIC.
all	Displays statistics for all asics or nodes.
location	Specifies the target location; the node-id is expressed in the R/S/I/P format.

Command Default

None

Command Modes

Administration EXEC

Command History

Release	Modification
Release 6.0.0	This command was first introduced.
Release 6.0.1	The **asic-type** keyword was added.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
sfe	read

Example

This example shows how to use the **show controller sfe statistics** command:

```
sysadmin-vm:0_RP0# show controller sfe statistics asic-type FE1600 block DCH instance 0
location 0/FC0
Wed Apr  20 06:40:33.225 UTC
DCH statistics:
---------------------------------
DCH0 FifoDiscardCounterP:                          0
DCH0 DCHReordDiscardCounterP:                      6
DCH0 FifoDiscardCounterS:                          0
DCH0 DCHReordDiscardCounterS:                      6
DCH0 UnreachDestCntP:                              0
DCH0 UnreachDestCntS:                              0
DCH0 DchDroppedLowMulCntP:                         0
DCH0 DchDroppedLowMulCntS:                         0
DCH0 ErrorFilterCntAP:                             0
DCH0 ErrorFilterCntBP:                             0
DCH0 ErrorFilterCntAS:                             0
DCH0 ErrorFilterCntBS:                             0
DCH0 DropLowPriCntP:                               0
DCH0 DropLowPriCntS:                               0
DCH0 Ecc_1bErrCnt:                                 0
DCH0 Ecc_2bErrCnt:                                 0
DCH0 ParityErrCnt:                                 0
DCH1 FifoDiscardCounterP:                          0
DCH1 DCHReordDiscardCounterP:                     18
DCH1 FifoDiscardCounterS:                          0
DCH1 DCHReordDiscardCounterS:                     18
DCH1 UnreachDestCntP:                              0
DCH1 UnreachDestCntS:                              0
DCH1 DchDroppedLowMulCntP:                         0
DCH1 DchDroppedLowMulCntS:                         0
DCH1 ErrorFilterCntAP:                             0
DCH1 ErrorFilterCntBP:                             0
DCH1 ErrorFilterCntAS:                             0
DCH1 ErrorFilterCntBS:                             0
DCH1 DropLowPriCntP:                               0
DCH1 DropLowPriCntS:                               0
DCH1 Ecc_1bErrCnt:                                 0
DCH1 Ecc_2bErrCnt:                                 0
DCH1 ParityErrCnt:                                 0
DCH2 FifoDiscardCounterP:                          0
DCH2 DCHReordDiscardCounterP:                      0
DCH2 FifoDiscardCounterS:                          0
DCH2 DCHReordDiscardCounterS:                      0
DCH2 UnreachDestCntP:                              0
DCH2 UnreachDestCntS:                              0
DCH2 DchDroppedLowMulCntP:                         0
DCH2 DchDroppedLowMulCntS:                         0
```

```
DCH2 ErrorFilterCntAP:                          0
DCH2 ErrorFilterCntBP:                          0
DCH2 ErrorFilterCntAS:                          0
DCH2 ErrorFilterCntBS:                          0
DCH2 DropLowPriCntP:                            0
DCH2 DropLowPriCntS:                            0
DCH2 Ecc_1bErrCnt:                              0
DCH2 Ecc_2bErrCnt:                              0
DCH2 ParityErrCnt:                              0
DCH3 FifoDiscardCounterP:                       0
DCH3 DCHReordDiscardCounterP:                   0
DCH3 FifoDiscardCounterS:                       0
DCH3 DCHReordDiscardCounterS:                   0
DCH3 UnreachDestCntP:                           0
DCH3 UnreachDestCntS:                           0
DCH3 DchDroppedLowMulCntP:                      0
DCH3 DchDroppedLowMulCntS:                      0
DCH3 ErrorFilterCntAP:                          0
DCH3 ErrorFilterCntBP:                          0
DCH3 ErrorFilterCntAS:                          0
DCH3 ErrorFilterCntBS:                          0
DCH3 DropLowPriCntP:                            0
DCH3 DropLowPriCntS:                            0
DCH3 Ecc_1bErrCnt:                              0
DCH3 Ecc_2bErrCnt:                              0
DCH3 ParityErrCnt:                              0
```

show platform

To display information and status for each node in the system, use the **show platform** command in EXEC mode or Administration EXEC mode.

show platform [**node-id**]

Syntax Description

node-id	Node for which information needs to be displayed. Node-id needs to be entered in R/S/I/P format.

Command Default

None

Command Modes

EXEC or Admin EXEC

Command History

Release	Modification
Release 5.2.4	This command was introduced.
Release 6.0.1	The display output has been modified to display additional details for line cards.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The show platform command provides a summary of the nodes in the system, including node type and status.

Task ID

Task ID	Operation
system	read

Example

This example shows how to use the **show platform** command:

```
RP/0/RP1:router # show platform

Node              Type                       State             Config state
--------------------------------------------------------------------------------
0/0/CPU0          NCS4K-2H10T-OP-KS          IOS XR RUN        NSHUT
0/1/CPU0          NCS4K-2H10T-OP-KS          IOS XR RUN        NSHUT
0/2/CPU0          NCS4K-20T-O-S              IOS XR RUN        NSHUT
0/4/CPU0          NCS4K-2H-O-K               IOS XR RUN        NSHUT
0/5/CPU0          NCS4K-2H10T-OP-KS          IOS XR RUN        NSHUT
0/6/CPU0          NCS4K-20T-O-S              IOS XR RUN        NSHUT
0/8/CPU0          NCS4K-20T-O-S              IOS XR RUN        NSHUT
0/9/CPU0          NCS4K-2H10T-OP-KS          IOS XR RUN        NSHUT
0/10/CPU0         NCS4K-20T-O-S              IOS XR RUN        NSHUT
0/11/CPU0         NCS4K-20T-O-S              IOS XR RUN        NSHUT
0/12/CPU0         NCS4K-2H-O-K               IOS XR RUN        NSHUT
0/13/CPU0         NCS4K-20T-O-S              IOS XR RUN        NSHUT
0/15/CPU0         NCS4K-20T-O-S              IOS XR RUN        NSHUT
0/RP0/CPU0        NCS4K-RP                   IOS XR RUN        NSHUT
```

```
0/RP1/CPU0       NCS4K-RP                 IOS XR RUN       NSHUT
0/FC0            NCS4016-FC2-M            OPERATIONAL      NSHUT
0/FC1            NCS4016-FC2-M            OPERATIONAL      NSHUT
0/FC2            NCS4016-FC2-M            OPERATIONAL      NSHUT
0/FC3            NCS4016-FC2-M            OPERATIONAL      NSHUT
0/FT0            NCS4K-FTA                FAILED           NSHUT
0/FT1            NCS4K-FTA                FAILED           NSHUT
0/PT1            NCS4K-AC-PEM             OPERATIONAL      NSHUT
0/EC0            NCS4K-ECU                OPERATIONAL      NSHUT
```

Interface GCC Command Reference

This chapter describes commands to configure the Interface GCC.

interface gcc0

To enter the configuration mode of GCC interface on an OTUk controller, use the **interface gcc0** command in the config mode.

interface gcc0 [*R/S/I/P*]

Syntax Description

R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

Disable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to enter the configuration mode of GCC interface on an OTU controller:

```
RP/0/RP0:hostname(config)# interface gcc0 0/0/0/0
```

interface gcc1

To enter the configuration mode of GCC interface on an ODUk controller, use the **interface gcc1** command in the config mode. To delete the controller oduk, use the **no** form of this command.

interface gcc1 [*R/S/I/P*]
no interface gcc1 [*R/S/I/P*]

Syntax Description

gcc1	Enters the configuration mode.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

Disable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to enter the configuration mode of GCC interface on an ODU controller.

```
RP/0/RP0:hostname (config)# interface gcc1 0/0/0/0
```

ipv4 address odu

To configure IP address for GCC on an ODUk controller, use the **ipv4 address** command in the config mode. To delete this feature, use the **no** form of this command.

ipv4 address
no ipv4 address

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure IP address for GCC1 on the ODU controller.

```
RP/0/RP0:hostname (config-if)# ipv4 address 1.1.1.1/24
```

ipv4 address otu

To configure IP address for GCC on an OTUk controller, use the **ipv4 address** command in the config mode. To delete this feature, use the **no** form of this command.

ipv4 address
no ipv4 address

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure IP address for GCC1 on the OTU controller.

```
RP/0/RP0:hostname (config-if)# ipv4 address 1.1.1.1/24
```

show interfaces

To display IP address and status of all the interfaces, use the **show interfaces** command in the exec mode.

show interfaces

This command has no keywords or arguments.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

This example shows how to display IP address and brief status of all the interfaces:

```
RP/0/RP0:hostname # show ip interfaces
```

```
Wed Jan  5 05:04:46.659 UTC
Interface                      IP-Address      Status                Protocol
GCC00/0/0/0                    1.1.1.1         Up                    Down
MgmtEth0/RP1/CPU0/0            unassigned      Shutdown              Down
```

show interfaces gcc0

To display all the interfaces on which GCC is configured, use the **show interfaces gcc0** command in the exec or config mode.

show interfaces gcc0 [*R/S/I/P*]

Syntax Description

R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Modes

Exec mode

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

This example shows how to display all the interfaces on which GCC is configured:

```
RP/0/RP0:hostname # show interfaces gcc0 0/1/0/0
```

```
GCC00/1/0/0 is up, line protocol is up
  Interface state transitions: 2
  Hardware is GCC0
  Internet address is 1.1.1.1/24
  MTU 4474 bytes, BW 4294967295 Kbit (Max: 4294967295 Kbit)
     reliability Unknown, txload Unknown, rxload Unknown
  Encapsulation PPP,  loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP
  Last input Unknown, output Unknown
  Last clearing of "show interface" counters Unknown
  Input/output data rate is disabled
```

show interfaces gcc1

To display all the interfaces on which GCC is configured, use the **show interfaces gcc1** command in the exec mode.

show interfaces gcc1 [*R/S/I/P*]

Syntax Description

show gcc1	Shows the gcc1 configuration mode.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

The following example shows how to display all the interfaces on which GCC is configured.

```
RP/0/RP0:hostname # show ip interface brief gcc1 0/2/0/1
```

```
GCC10/2/0/1 is up, line protocol is up
  Interface state transitions: 2
  Hardware is GCC1
  Internet address is 1.2.3.4/24
  MTU 4474 bytes, BW 4294967295 Kbit (Max: 4294967295 Kbit)
     reliability Unknown, txload Unknown, rxload Unknown
  Encapsulation PPP,  loopback not set, keepalive set (10 sec)
  LCP Open
  Req-Sent: IPCP
  Last input Unknown, output Unknown
  Last clearing of "show ip interface brief" counters Unknown
  Input/output data rate is disabled
```

Protection Command Reference

This chapter describes the commands to protect the ODUk controllers.

controller odu-group-mp

To create an ODU group controller, use the **controller odu-group-mp** command in the config mode. To delete an ODU group controller, use the **no** form of this command.

controller odu-group-mp *Group-ID* {**signal**} [**otn** | **sonet** | **ethernet**] {**odu-type**} *type-of-the-odu* [**protecting-controller** | **protection-attributes** | **protection-switching** | **working-controller**] [**connection-mode** | **protection-mode** | **protection-type** | **timers**] *mode-of-the-connection*

no controller odu-group-mp *Group-ID* {**signal type**} *type-of-the-odu*

Syntax Description

Group ID	Identifier of the ODU group controller. The valid range is from 1 to 65535.
signal	Configures the type of the client signal to be added in the ODU group controller.
odu-type	Configures the odu-type of the signal selected for the ODU group controller.
Type of the ODU	Displays the odu-type of the signal selected for the ODU group controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to create an ODU group controller:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 4 signal sonet odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp4)# protecting-controller odu1 0/0/0/1
RP/0/RP0:hostname(config-odu-group-mp4)# working-controller odu1 0/0/0/1
```

odu-group

To configure protection switch on an ODU group controller use the **odu-group** command in the exec or config mode. To delete an ODU group controller, use the **no** form of this command.

odu-group [**mp** | **te**] *Group ID* [**clear odu-dest** | **exercise** | **forced odu-dest** | **manual odu-dest**] *ODUk R/S/I/P*

Syntax Description

mp	Configures the protection switch on an ODU group controller pertaining to the management plane.
te	Configures the protection switch on an ODU group controller pertaining to the control plane.
Group ID	Identifier of the ODU group controller. The valid range is from 1 to 65535.
clear	Clears the protection switch.
odu-dest	Configures the protection switch on the specified controller.
exercise	Checks if an ODU group controller is ready for the protection switch.
forced odu-dest	Performs forced switch.
manual odu-dest	Performs manual switch.
ODUk	Name of the controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller

Command Default

None

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure a forced switch:

```
RP/0/RP0:hostname(config)# odu-group mp 1 forced odu-dest odu2 0/2/0/1/22
```

working-controller

To configure an ODUk controller as the working controller in the ODU group controller, use the **working-controller** command in the config mode. To delete an ODUk controller as the working controller in the ODU group controller, use the **no** form of this command.

working-controller [*ODUk R/S/I/P*]
no working-controller [*ODUk R/S/I/P*]

Syntax Description

ODUk	Name of the ODUk controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure an ODU1 controller as the working controller in the ODU group 1 controller:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 1 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp 1)# working-controller odu1 0/0/0/0
```

protecting-controller

To configure an ODUk controller as the protecting controller in the ODU group controller, use the **protecting-controller** command in the config mode. To delete an ODUk controller as the protecting controller in the ODU group controller, use the **no** form of this command.

protecting-controller [*ODUk R/S/I/P*]

no protecting-controller [*ODUk*]

Syntax Description

ODUk	Name of the ODUk controller.
Rack/Slot/Instance/Port	Interface instance of the controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure an ODU1 controller as the protecting controller in the ODU group 1 controller:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 1 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp 1)# protecting-controller odu1 0/0/0/1
```

protection-attributes connection-mode

To configure connection mode of all the protecting controllers in the ODU Group controller, use the **protection-attributes connection mode** command in the config mode. To delete a connection mode of all the protecting controllers in the ODU Group controller, use the **no** form of this command.

SNC _I indicates that the protection is provided in the case of a fabric cut and signal degrade.

SNC _N indicates that the protection is provided in the case of a fiber cut.

SNC_S indicates that the protection is provided in the case of server layer failures.

protection-attributes connection mode [{**snc-i** | **snc-n** | **snc-s**}{ **tcm-id**}] *ID*

no protection-attributes connection mode [{**snc-i** | **snc-n** | **snc-s**}{ **tcm-id**}] *ID*

Syntax Description

snc-i	Configures the inherent subnetwork connection.
snc-n	Configures the subnetwork connection.
snc-s	Configures the subnetwork connection.
tcm-id	Configures the tandem connection monitoring. This option is valid for SNC-s mode.
ID	Identifier of the TCM connection. The valid range is from 1 to 6.

Command Default

SNC-N

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the connection mode of an ODU group controller as inherent subnetwork connection:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 1 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-attributes connection-mode snc-i
```

protection-attributes protection-mode

To configure protection mode of all the protecting controllers in the ODU Group controller, use the **protection-attributes protection-mode** command in the config mode. To delete a protection mode of all the protecting controllers in the ODU Group controller, use the **no** form of this command.

protection-attributes protection-mode [**nonrevertive** | **revertive** | **wait-to-restore-time**] *timer*
no protection-attributes protection-mode [**nonrevertive** | **revertive** | **wait-to-restore-time**] *timer*

Syntax Description

nonrevertive	Configures the non-revertive protection mode.
revertive	Configures the revertive protection mode.
wait-to-restore	Configures the wait-to-restore timer in the revertive mode.
Timer	Configures the range of wait-to-restore timer. The valid range is from 300 to 720 seconds.

Command Default

0

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the protection mode of an ODU group controller as revertive and nonrevertive:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 1 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp1)# protection-attributes protection-mode revertive
wait-to-restore-time 315
RP/0/RP0:hostname(config-odu-group-mp1)# protection-attributes protection-mode nonrevertive
```

protection-attributes protection-type

To configure protection type of all the protecting controllers in the ODU Group controller, use the **protection-attributes protection-type** command in the config mode. To delete a protection type of all the protecting controllers in the ODU Group controller, use the **no** form of this command.

protection-attributes protection-type [**APSbidi** | **APSuni** | **noAPSuni**]
no protection-attributes protection-type [**APSbidi** | **APSuni** | **noAPSuni**]

Syntax Description

APSbidi	Configures the 1+1 bi-directional automatic protection switching.
APSuni	Configures the 1+1 unidirectional automatic protection switching.
noAPSuni	Configures the no APS protocol in unidirectional protection switch.

Command Default

OTM_PROT_TYPE_ONE_PLUS_ONE_APS_BIDI

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the protection type of an ODU group controller as 1+1 unidirectional automatic protection switching:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 1 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-attributes protection-type APSuni
```

protection-attributes timers

To configure hold-off timer for the ODU Group controller, use the **protection-attributes timers** command in the config mode. To delete a hold-off timer for the ODU Group controller, use the **no** form of this command.

protection-attributes timers {**hold-off-time**} *timer*
no protection-attributes timers protection-attributes timers {**hold-off-time**} *timer*

Syntax Description

hold-off-time	Configures the hold-off timer.
timer	Configures the range of hold-off time in multiple of hundred mili seconds. The valid range is from 100 to 10000.

Command Default

0

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the hold-off timer for the ODU group controller:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 1 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-attributes timers hold-off-time 100
```

protection-switching

To configure a controller as a locked out resource in an ODU Group controller, use the **protection-switching** command in the config mode. To delete a controller as a locked out resource in an ODU Group controller, use the **no** form of this command.

protection-switching { **operate lockout odu-dest** } [*ODUk R/S/I/P*]
no protection-switching { **operate lockout odu-dest** } [*ODUk R/S/I/P*]

Syntax Description

operate	Configures the protection switching.
lockout	Configure a controller as a locked out resource.
odu-dest	Specifies a controller to be locked out.
ODUk	Name of the ODUk controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

ODU group is always created on head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure a protecting controller as a locked out resource:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 1 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-switching operate lockout odu-dest
odu0 0/0/0/0
```

show controllers [odu-group-mp | odu-group-te]

To display details of an ODU group controller, use the **show controller [odu-group-mp | odu-group-te]** command in the exec mode.

show controllers [**odu-group-mp** | **odu-group-te**] *Group ID* [**protection-detail** | **xc**]

Syntax Description

odu-group-mp	Displays details of the ODU group controller pertaining to management plane.
odu-group-te	Displays details of the ODU group controller pertaining to control plane.
Group ID	Identifier of the ODU group controller.
protection-detail	Displays the hardware information of the ODU group controller.
xc	Displays the cross connect details of the ODU group controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

This example shows how to display the details of an ODU group controller pertaining to management plane:

```
RP/0/RP0:hostname # show controllers ODU-group-mp 1
```

```
ODU Group Information
----------------------------------------------------------------
ODU GROUP ID                                    : 1
Controller State                                : Up

 WORKING CONTROLLER
```

```
ODU NAME                                              : ODU1 0/0/0/1
ODU ROLE                                              :  WORKING
ODU STATE                                             :  Not present

 PROTECTED CONTROLLER

ODU NAME                                              :  NOT SET
ODU ROLE                                              :  NOT SET
ODU STATE                                             :  Not present

 RESTORED CONTROLLER

ODU NAME                                              :  NOT SET
ODU ROLE                                              :  NOT SET
ODU STATE                                             :  Not present

PROTECTION PARAMETERS :
Connection Mode                                       : SNC_N
Protection Type                                       : 1+1 Bidirectional Protection
Tcmid                                                 : 0
Protection Mode                                       : Non-Revertive
Hold off timer                                        : 0
Wait-to-restore timer                                 : 300

RESTORATION PARAMETERS :
Restoration Mode                                      : Non-Revertive

LOCKOUT                                               : NO
SWITCH OVER                                           : NO_SWITCHOVER
```

Example

This example shows how to display the details of an ODU group controller pertaining to management plane:

```
RP/0/RP0:hostname # show controllers ODU-group-te 12
```

```
Thu Jul 31 15:28:51.191 UTC

ODU Group Information
-----------------------------------------------------------------
ODU GROUP ID : 12
Controller State : Down

WORKING CONTROLLER

ODU NAME : NOT SET
ODU ROLE : NOT SET
ODU STATE : Not present
GMPLS Request Context Data
Request Time :
Context Type : NONE
RM Type : NONE
Tunnel Info Type : NONE
GMPLS Request Context Data
Request Time :
Context Type : NONE
RM Type : NONE
Tunnel Info Type : NONE

PROTECTED CONTROLLER
```

```
ODU NAME : NOT SET
ODU ROLE : NOT SET
ODU STATE : Not present
GMPLS Request Context Data
Request Time :
Context Type : NONE
RM Type : NONE
Tunnel Info Type : NONE
GMPLS Request Context Data
Request Time :
Context Type : NONE
RM Type : NONE
Tunnel Info Type : NONE

RESTORED CONTROLLER

ODU NAME : NOT SET
ODU ROLE : NOT SET
ODU STATE : Not present
GMPLS Request Context Data
Request Time
-----------------------------------------------
31 15:31:47.967 IST
```

Example

This example shows how to display the details of an ODU group controller pertaining to management plane:

```
RP/0/RP0:hostname # show controllers ODU-group-mp 1
```

```
ODU Group Information
-------------------------------------------------------------
ODU GROUP ID                                  : 1
Controller State                              : Up

 WORKING CONTROLLER

ODU NAME                                      : ODU1 0/0/0/1
ODU ROLE                                      :  WORKING
ODU STATE                                     :  Not present

 PROTECTED CONTROLLER

ODU NAME                                      :  NOT SET
ODU ROLE                                      :  NOT SET
ODU STATE                                     :  Not present

 RESTORED CONTROLLER

ODU NAME                                      :  NOT SET
ODU ROLE                                      :  NOT SET
ODU STATE                                     :  Not present

PROTECTION PARAMETERS :
Connection Mode                               : SNC_N
Protection Type                               : 1+1 Bidirectional Protection
Tcmid                                         : 0
Protection Mode                               : Non-Revertive
Hold off timer                                : 0
Wait-to-restore timer                         : 300
```

```
RESTORATION PARAMETERS :
Restoration Mode                                 : Non-Revertive

LOCKOUT                                          : NO
SWITCH OVER                                      : NO_SWITCHOVER
```

Example

This example shows how to display the details of an ODU group controller pertaining to management plane:

```
RP/0/RP0:hostname # show controllers ODU-group-mp1 xc
```

```
xconnect id                                      : 1
xconnect Name                                    :
FWD ref                                          : ODU1 0/0/0/3
FWD ref.ifhandle                                 : 4736
Owner                                            : MP
Resource State                                   : ODG Cross Connection
ODU STATE                                        : Not present
Local Failure                                    : No
Remote Failure                                   : No

Xconnect Status                                  : DP programmed
```

Cross Connect Command Reference

This chapter describes the commands to create cross connection between the controllers.

xconnect

To create a cross connection between controllers, use the **xconnect** command in the global configuration mode. To delete a cross connect, use the **no xconnect** command in the global configuration mode.

xconnect *ID* **endpoint-1** *ODUk R/S/I/P* **endpoint-2** *ODUk R/S/I/P*

xconnect *ID* **endpoint-1 odu-grp-mp** *Group ID* **endpoint-2 Odu-grp-mp** *Group ID*

xconnect *ID* **endpoint-1 Odu-grp-mp** *Group ID* **endpoint-2** *ODUk R/S/I/P*

no xconnect *ID*

Syntax Description

ID	Enter the cross connect ID. The valid range of cross connect ID is from 1 to 32655.
endpoint-1	Creates a cross connection from the endpoint of the first ODU controller.
endpoint-2	Creates a cross connection to the endpoint of the second ODU controller.
R/S/I/P	Interface instance of the controller.
Group ID	ID of the ODU group controller.
ODUk	Name of the controller.
Odu-grp-mp	Creates a cross connection from the ODU group controller.

Command Modes

Global configuration (config).

Command History

Release	Modification
5.2.1	This command was introduced.

Usage Guidelines

You can create a cross connection between similar types of ODUk controllers. For example: ODU1 to ODU1.

Two endpoints cannot be cross connected on the same port.

Example

The following example shows how to create a cross connection between ODUk to ODUk .

```
Router (config)#xconnect 2 endpoint-1 ODU1 0/0/0/1 endpoint-2 ODU2 0/0/0/2
```

The following example shows how to create a cross connection between one ODU Group to another ODU Group.

```
Router (config)#xconnect 4 endpoint-1 odU-grp-mp 4 endpoint-2 odU-grp-mp 3
```

The following example shows how to create a cross connection between ODU Group to ODUk .

```
Router (config)#xconnect 5 endpoint-1 odU-grp-mp 4 endpoint-2 odU1 0/0/0/1
```

The following example shows how to delete a cross connection.

```
Router (config)# no xconnect 2
```

show xconnect

To show details of a cross connection, use the **show xconnect** command in the privileged mode. To show all the cross connections, use the **show xconnect all** command in the privileged mode.

show xconnect *ID*

show xconnect all

Syntax Description

ID	Displays the cross connection ID. The valid range of cross connection ID is from 1 to 32655.
all	Displays all the cross connections.

Command Modes

Privileged (#)

Command History

Release	Modification
5.2.1	This command was introduced.

Example

The following example shows how to display description of a cross connection using its ID.

```
Router # show xconnect 1
```

```
Thu Oct  3 12:27:19.409 IST

Xconnect information for static permanent connection
-----------------------------------------------------

Xconnect Id     Endpoint First     Endpoint Second      status
    1            ODU10_0_0_0        ODU10_0_0_1      DP programmed
```

The following example shows how to display all the cross connections.

```
Router # show xconnect all
```

```
Thu Oct  3 12:27:00.986 IST

Xconnect information for static permanent connection
-----------------------------------------------------

Xconnect Id     Endpoint First      Endpoint Second       status
    1             ODU10_0_0_0         ODU10_0_0_1       DP programmed

    7             ODU10_0_0_1          ODU40_0_0_4       DP not programmed
```

GMPLS Command Reference

This chapter describes the commands to configure the GMPLS.

affinity-map

To define global name-to-value mapping, use the **affinity-map** command in config mode.

affinity map <*colour*> **bit-position** <*bit-position*>

Syntax Description

colour	Enters the colour like red, blue, green.
bit-position	Enters bit position. Valid value range is 0-31

Command Modes

Config mode

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Task ID

Task ID	Operation
ouni	write

Example

The following example shows how to define an affinity map:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# affinity-map red bit-position 1
RP/0/RP0:hostname(config-te-gmpls-nni)# affinity-map green bit-position 0
```

affinity-name

To assign one or multiple colours to the OTN link , use the **affinity-name** command in config mode. To disable affinity-name, use the **no** form of this command.

affinity name <*color*> <*color*>…<*color*> *upto 32 colors*

Syntax Description

color	Enters the colour like red, blue, green.

no affinity name

Command Modes

Config mode

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Task ID

Task ID	Operation
ouni	write

Example

The following example shows how to assign multiple colours to the OTN link:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni
RP/0/RP0:hostname(config-te-gmpls-nni)# topology instance ospf abc area 5
RP/0/RP0:hostname(config-te-gmpls-nni-ti)# controller otu4 0/0/0/1
RP/0/RP0:hostname(config-te-gmpls-nni-ti-cntl)# affinity-name red blue green yellow
```

announce srlg

To pass on the SRLG from OTN layer to packet interfaces, use the **announce srlg** command in config mode. To disable announcing SRLG, use the **no** form of this command.

announce srlg

no announce srlg

Command Modes

Config mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operation
ouni	write

Example

The following example shows how to configure SRLG announcement on Ethernet Terminated ODU:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni
RP/0/RP0:hostname(config-te-gmpls-nni)# controller odu-group-te 10
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# signalled-bandwidth ODU2
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# static-uni local-termination interface-name
TenGigE0/1/0/0/100 remote-termination unnumbered 32
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# destination ipv4 unnumbered 10.77.132.185
interface-if index 19
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# announce srlg
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# path-option 1 dynamic protected-by none lockdown
```

announce srlgs

To announce all SRLGs discovered through GMPLS signaling to RSI (Router Space Infrastructure), use the **announce srlgs** command in MPLS-TE GMPLS UNI controller mode. To disable announcing SRLGs to RSI, use the **no** form of this command.

announce srlgs

no announce srlgs

Command Default None

Command Modes MPLS-TE GMPLS UNI controller configuration

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines None

Task ID

Task ID	Operation
mpls-te	read, write
ouni	read, write

Example

The following example shows how to configure SRLG announcement:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-uni
RP/0/RP0:hostname(config-te-gmpls-uni)# controller optics 0/1/0/2
RP/0/RP0:hostname(config-te-gmpls-cntl)# announce srlgs
```

area ID

To configure the area ID of the ospf interface, use the **area** command in the config mode. To delete the area ID of the ospf, use the **no** form of this command.

area [*ID value*]

no area [*ID value*]

Syntax Description

area	Configures the area ID of the OSPF interface.
value	Displays the area ID of the OSPF interface.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the area ID of the OSPF interface:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
```

attribute-set

To create attribute-set that defines affinity constraints, use the **attribute-set** command in config mode.

attribute-set path-option <*name*>
affinity <*constraint*>

Syntax Description

name	Name of the attribute-set.
constraint	• include : Specifies that the TE link will be eligible for path-calculation if it has all the colours listed in the constraint. The link may have additional colours. • include-strict : Specifies that the TE link will be eligible for path-calculation only if it has the same set of colours listed in the constraint. The link should not have any additional colour. • exclude: Specifies that the TE link will be eligible for path-calculation if it does not have all the colours listed in the constraint. • exclude-all: This constraint is not associated with any colour.If this constraint is configured for a tunnel, path-calculator will only accept the links that do not have any colour.

Command Modes

Config mode

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Task ID

Task ID	Operation
ouni	write

Example

The following example shows how to define an attribute set:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# attribute-set path-option Affinity1
RP/0/RP0:hostname(config-te-attribute-set)# affinity include red
```

attribute-set xro

To configure the xro attribute set for circuit diversity, use the **attribute-set xro** command in the config mode. To delete an attribute set use the **no** form of this command.

attribute-set xro [*attribute set name*] **exclude strict lsp source** [*head node IP address*] **destination** [*tail node IP address*] **tunnel-id** [*tunnel_id*] **extended-tunnel-id** [*ext_tunnel_id*]
no attribute-set xro [*attribute set name*]
attribute-set xro [*attribute set name*] **no exclude strict lsp source** [*head node IP address*] **destination** [*tail node IP address*] **tunnel-id** [*tunnel_id*] **extended-tunnel-id** [*ext_tunnel_id*]

Syntax Description

exclude	Specifies path to be excluded for circuit diversity.
strict	Specifies that diverse circuit will come up only if the conditions specified under exclusion are met.
lsp	Specify path-diversity from another LSP.
source	Specifies the IP address of head node in circuit whose diverse circuit you want to create.
destination	Specifies the IP address of tail node in circuit whose diverse circuit you want to create.
tunnel-id	Specifies the tunnel Id of circuit whose diverse circuit you want to create.
extended-tunnel-id	Specifies the extended-tunnel-id of circuit whose diverse circuit you want to create. This is same as head node IP address.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to define xro attribute set for creating a diverse circuit.

```
RP/0/RP0/CPU0:router(config)# attribute-set xro Xro_nni1_div_tun0 exclude strict lsp source
```

```
 192.168.0.1 destination 192.168.0.2 tunnel-id 0 extended-tunnel-id 192.168.0.1

RP/0/RP0/CPU0:router(config)# no attribute-set xro Xro_nni1_div_tun0

RP/0/RP0/CPU0:router(config)# attribute-set xro Xro_nni1_div_tun0 no exclude strict lsp
source 192.168.0.1 destination 192.168.0.2 tunnel-id 0 extended-tunnel-id 192.168.0.1
```

controller odu-group-te

To create an ODU group controller, use the **controller odu-group-te** command in the config mode. To delete ODU group controller, use the **no** form of this command.

controller odu-group-te [*Group ID*]
no controller odu-group-te [*Group ID*]

Syntax Description

Groupr ID	Identifier of the ODU group Controller. The valid range is from 0 to 64535.

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Controller odu-group-te has information for GMPLS tunnel only.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to create ODU Group controller.

```
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname (config-mpls-te)# gmpls optical-nni
RP/0/RP0:hostname (config-te-gmpls-nni)# controller odu-group-te 1
```

destination

To create destination of GMPLS OTN tunnel, use the **destination** command in the config mode. To delete the destination for an odu-group-te controller, use the **no** form of this command.

destination {**ipv4 unicast**} *A.B.C.D*
no destination {**ipv4 unicast**} *A.B.C.D*

Syntax Description

destination	Specifies the destination of the GMPLS OTN tunnel.
ipv4	Specifies an IPv4 destination.
unicast	Specifies an IPv4 unicast destination.
A.B.C.D	Specifies the tunnel destination address.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Destination is used define the destination of the nni to nni tunnel. Destination of the tunnel is identified by the tail node Id of the router.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to configure destination for an odu-group-te controller.

```
RP/0/RP0:hostname(config-gmpls-tun-0x1)# destination ipv4 unicast 1.2.3.4
```

explicit-path

To configure an explicit path, use the **explicit-path** command in the config mode. To delete an explicit-path use the **no** form of this command.

explicit-path { **name** | **identifier** } [*name* | *id_value*] **index** *index_val* **next-address** { **strict** | **loose** } **ipv4 unicast ip_address** *router_id*
explicit-path { **name** | **identifier** } [*name* | *id_value*] **index** *index_val* **next-address** { **strict** | **loose** } **ipv4 unicast ip_address unnumbered** *link_address*
no explicit-path { **name** | **identifier** } [*name* | *id_value*]
explicit-path { **name** | **identifier** } [*name* | *id_value*] **no index** *index_val*

Syntax Description

name	Specifies name of the explicit path.
identifier	Specifies unique identifier of the explicit path.
index	Uniquely identifies each next hop entry in an explicit-path. Also it specifies the order in which the hop entries will be processed. The lowest index shall be processed first.
next-address	Specifies next hop address.
strict	Specifies that next hop must be reached using a specified path.
loose	Specifies that next-hop need to be reached using any of the available paths.
ipv4 unicast	Specifies an IPv4 unicast next hop.
ip_address	Specifies next hop IP address.
unnumbered	Specifies that next hop is an unnumbered link. An unnumbered link is identified using router id and interface index.
name	Defines explicit path name.
id_value	Defines explicit path id. The valid range for explicit path id is from 1 to 65535.
index_val	Defines a unique id for a next hop entry. The valid range for next hop index is from 1 to 65535.

link_address	Defines ip_address of next hop link.
router_id	Defines ip_address of next hop node.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to define explicit path for a circuit.

```
RP/0/RP0/CPU0:router(config)# explicit-path name Exp_path_OPT1_to_OPT5
index 10 next-address strict ipv4 unicast 1.1.1.1
index 20 next-address loose ipv4 unicast unnumbered 1.1.1.2 200

RP/0/RP0/CPU0:router(config)# explicit-path identifier 65
index 1 next-address strict ipv4 unnumbered unicast 1.1.1.2 50
index 2 next-address loose ipv4 unicast 1.1.1.1
```

gmpls optical-nni

To create a network-to-network interface (NNI), use the **gmpls optical-nni** command in the config mode. To delete NNI interface, use the **no** form of this command.

mpls traffic-eng
gmpls optical-nni
no gmpls optical-nni

Syntax Description

gmpls	Configures the routing protocol.
optical-nni	Specifies the network-network interface.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This sub mode causes the CLI prompt to change from "config-mpls-te" to “config-te-gmpls”. When you remove the gmpls optical-nni sub mode, it removes the entire configuration in it (as for any other parser sub mode) and the immediate destruction of all GMPLS tunnels.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to create NNI interface:

```
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname (config-mpls-te)# gmpls optical-nni
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni topology instance ospf OTN area 0
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni controller OTU40/2/0/0
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni controller tti-mode otu-sm
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni controller tti-mode otu admin-weight
1

RP/0/RP0:19#show running-config

 Building configuration...
!! IOS XR Configuration version = 5.2.3.13L
!! Last configuration change at Sun Jan 18 10:03:02 2015 by root
```

```
!
hostname 19
logging buffered debugging
telnet vrf default ipv4 server max-servers 99
username root
 group root-lr
 group cisco-support
 secret 5 $1$1DQO$diVcoqlNPwQMGpHfsAHVk.
!
explicit-path name protect-path
 index 1 next-address strict ipv4 unicast unnumbered 1.1.1.2 11
 index 2 next-address strict ipv4 unicast unnumbered 1.1.1.4 7
!
line console
 exec-timeout 0 0
!
vty-pool default 0 99 line-template telnet
ntp
 server 10.78.161.100
!
interface Loopback0
 ipv4 address 1.1.1.13 255.255.255.255
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 10.78.161.31 255.255.255.0
!
interface MgmtEth0/RP0/EMS/0
 shutdown
!
interface MgmtEth0/RP0/CRAFT/0
 shutdown
!
controller Optics0/0/0/3
 port-mode Otn framing opu2
!
controller Optics0/0/0/4
 port-mode SDH framing opu2 mapping bmp
!
controller Optics0/0/0/5
 port-mode Sonet framing opu2 mapping bmp
!
controller Optics0/0/0/14
 port-mode Otn framing opu2
!
controller Optics0/0/0/15
 port-mode Ethernet framing opu2e mapping bmp
!
controller Optics0/0/0/16
 port-mode Otn framing opu2
!
controller Optics0/0/0/17
 port-mode Otn framing opu2
!
controller Optics0/0/0/18
 port-mode Otn framing opu2
!
controller Optics0/0/0/19
 port-mode Otn framing opu2
!
controller Optics0/2/0/0
 port-mode Otn framing opu4
!
controller Optics0/2/0/1
 port-mode Otn framing opu4
```

```
!
controller Optics0/5/0/12
 port-mode Ethernet framing opu0 mapping gmp
!
controller Optics0/5/0/13
 port-mode Ethernet framing opu0 mapping gmp
!
controller OTU40/2/0/0
 gcc0
 secondary-admin-state normal
!
controller OTU40/2/0/1
 gcc0
 secondary-admin-state normal
!
interface GCC00/2/0/0
 ipv4 unnumbered Loopback0
!
interface GCC00/2/0/1
 ipv4 unnumbered Loopback0
!
router static
 address-family ipv4 unicast
  0.0.0.0/0 10.78.161.1
 !
!
router ospf OTN
 nsr
 router-id 1.1.1.13
 nsf ietf
 area 0
  mpls traffic-eng
  interface Loopback0
   passive disable
  !
  interface GCC00/2/0/0
   passive disable
  !
  interface GCC00/2/0/1
   passive disable
  !
 !
 mpls traffic-eng router-id 1.1.1.13
!
mpls traffic-eng
 attribute-set path-protection-aps APS
  timers
   wait-to-restore 300
  !
  sub-network connection-mode SNC-I
  protection-mode revertive
  protection-type 1-plus-1-UNIDIR-APS
 !
 attribute-set path-protection-aps New_Profile2
  sub-network connection-mode SNC-N
  protection-type 1-plus-1-BDIR-APS
 !
 attribute-set path-protection-aps New_Profile3
  timers
   wait-to-restore 300
  !
  sub-network connection-mode SNC-N
  protection-mode revertive
  protection-type 1-plus-1-BDIR-APS
```

```
!
attribute-set path-protection-aps New_Profile4
 timers
  wait-to-restore 300
 !
 sub-network connection-mode SNC-I
 protection-mode revertive
 protection-type 1-plus-1-BDIR-APS
!
gmpls optical-nni
 topology instance ospf OTN area 0
  controller OTU40/2/0/0
   tti-mode otu-sm
   admin-weight 1
  !
  controller OTU40/2/0/1
   tti-mode otu-sm
   admin-weight 1
  !
 !
 controller Odu-Group-Te 0
  signalled-name s1
  logging events lsp-status signalling-state
  logging events lsp-status switch-over
  logging events lsp-status cross-connect
  logging events lsp-status insufficient-bandwidth
  signalled-bandwidth ODU2e
  static-uni ingress-port controller TenGigECtrlr0/0/0/15 egress-port unnumbered 69
  destination ipv4 unicast 1.1.1.4
  path-protection attribute-set New_Profile4
  path-option 1 dynamic protected-by 2 lockdown
  path-option 2 dynamic lockdown
 !
 controller Odu-Group-Te 1
  signalled-name s2
  logging events lsp-status signalling-state
  logging events lsp-status switch-over
  logging events lsp-status cross-connect
  logging events lsp-status insufficient-bandwidth
  signalled-bandwidth ODU2
  static-uni ingress-port controller OTU20/0/0/14 egress-port unnumbered 68
  destination ipv4 unicast 1.1.1.4
  path-protection attribute-set New_Profile4
  path-option 1 dynamic protected-by none restored-from 3 lockdown
  path-option 3 dynamic lockdown
 !
 controller Odu-Group-Te 2
  signalled-name s3
  logging events lsp-status signalling-state
  logging events lsp-status switch-over
  logging events lsp-status cross-connect
  logging events lsp-status insufficient-bandwidth
  signalled-bandwidth ODU0
  static-uni ingress-port controller GigabitEthCtrlr0/5/0/12 egress-port unnumbered 56
  destination ipv4 unicast 1.1.1.4
  path-protection attribute-set New_Profile3
  path-option 1 dynamic protected-by 2 lockdown
  path-option 2 dynamic lockdown
 !
 controller Odu-Group-Te 3
  signalled-name s4
  logging events lsp-status signalling-state
  logging events lsp-status switch-over
  logging events lsp-status cross-connect
```

```
   logging events lsp-status insufficient-bandwidth
   signalled-bandwidth ODU2
   static-uni ingress-port controller OC1920/0/0/5 egress-port unnumbered 67
   destination ipv4 unicast 1.1.1.4
   path-protection attribute-set New_Profile4
   path-option 1 dynamic protected-by none restored-from 3 lockdown
   path-option 3 dynamic lockdown
  !
 !
!
xml agent tty
!
http server
```

gmpls optical-uni controller

To create a static uni xconnect, use the **gmpls optical-uni** command in the config mode. To delete an GMPLS controller, use the **no** form of this command.

static-uni {**ingress-port controller**} [*name-of-the-controller R/S/I/P*] {**egress-port unnumbered**} [*value*]

no static-uni {**ingress-port controller**} [*name-of-the-controller R/S/I/P*] {**egress-port unnumbered**} [*value*]

Syntax Description

static-uni	Specifies the static-uni of the tunnel.
ingress-port	Specifies the ingress port.
controller	Specifies the ingress port controller.
name-of-the-controller	Displays the name of the ingress controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller
egress-port	Specifies the egress port.
unnumbered	Specifies the tail-end customer port.
value	Enter the tail-end customer port IF index. Use **show snmp interface** command to see the IF index value that starts from 0 to 4294967295. Also, **snmp persist** command to the IF index value static. **Note** Refer the running configuration sample under **gmpls-optical-nni**.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to access the interface instance of an GMPLS optics controller on port2:

```
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-uni controller optics 0/0/0/2
```

interface gcc0

To configure the gcc0 on the ospf interface, use the **interface gcc0** command in the config mode. To delete the gcc0 on the ospf interface, use the **no** form of this command.

interface gcc0 [*R/S/I/P*]

no interface gcc0 [*R/S/I/P*]

Syntax Description

gcc0	Configures the general communication channel (GCC) on an OSPF interface.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the gcc0 on an ospf interface:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface gcc0 0/1/0/12
```

interface loopback

To configure the loopback on an ospf interface, use the **interface loopback** command in the config mode. To delete the loopback from an ospf interface, use the **no** form of this command.

interface loopback [*ID Value*]

no interface loopback [*ID Value*]

Syntax Description

loopback	Configures the loopback on an OSPF interface.
ID	Displays the loopback ID of the OSPF interface.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the loopback on an ospf interface:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface loopback 0
```

link-id

To configure the link identifier address of the LMP controller, use the **link-id** command in the config mode. To delete the link identifier address of the LMP controller, use the **no** form of this command.

link-id {**ipv4 unicast**} *value*

no link-id {**ipv4 unicast**} *value*

Syntax Description

ipv4	Configures the local link identifier address of the LMP controller.
unicast	Configures the unicast address of the LMP controller.
value	Displays the link identifier address of the LMP controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the local link identifier address of the LMP controller:

```
RP/0/RP0:hostname(config)# lmp gmpls optical-uni controller optics 0/0/0/2
RP/0/RP0:hostname(config-lmp-gmpls-uni-cntl)# link-id ipv4 unicast 1.2.3.4
```

lmp gmpls optical-uni controller

To configure an LMP controller, use the **lmp gmpls optical-uni** command in the config mode. To delete an LMP controller, use the **no** form of this command.

lmp gmpls optical-uni [**controller** | **neighbor** | **router-id**] *name-of-the-controller R/S/I/P*

no lmp gmpls optical-uni [**controller** | **neighbor** | **router-id**] *name-of-the-controller R/S/I/P*

Syntax Description

controller	Configures the lmp gmpls uni on a controller.
name-of-the-controller	Displays the name of the controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to access the interface instance of an LMP optics controller on port2:

```
RP/0/RP0:hostname(config)# lmp gmpls optical-uni controller optics 0/0/0/2
```

logging events lsp status state

To enable the logging events of lsp status state messages for logical and physical links, use the **logging events lsp status state** command in the config configuration mode. To delete this command, use the **no** form of this command.

logging events lsp-status state
no logging events lsp-status state

Syntax Description

logging	Enables the login event of Lsp status.
events	Specifies per interface logging events.
lsp-state	Enables interface LSP state changes alarms.
state	Enables interface LSP UP/DOWN changes alarms.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

There are three types of LSP: working, protected and restore. If working lsp is not configured properly at the initial setup then the other two lsps will also not be available. Selection of the same LSP (working/ protected) to pick traffic at the head and the tail end is performed by the hardware.

The switching line should be between 50 milliseconds from one LSP to the other.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to logging inside a controller for logging events lsp-status state:

```
RP/0/RP0/CPU0:router(config-te-gmpls-tun-0x7)# logging events lsp-status state
```

path option

To create a path option of GMPLS tunnel, use the **path-option** command in the config mode. To delete this behavior, use the **no** form of this command.

path-option [*path id*] {**explicit**} [*name* | *identifier*] **path name** [*lockdown* | *protected-by* | *restored-from*] [*restored from id*] [**lockdown** | **restored-from**] [*restored from id*] **lockdown**
path-option [*path id*] {**explicit**} [**name** | **identifier**] [*explicit path name* | *explicit path id*] [**xro-attribute-set**] [*xro attribute set name*] **lockdown verbatim**
path-option [*path id*] {**dynamic**} [*lockdown* | *protected-by* | *restored-from*] [*restored from id*] [**lockdown** | **restored-from**] [*restored from id*] [**xro-attribute-set**] [*xro attribute set name*] **lockdown**
path-option [*path id*] **no-ero** [**xro-attribute-set**] [*xro attribute set name*] **lockdown**
no path-option [*path id*]
no path-option [*id*] {**explicit**} [*name* | *identifier*] **path name** [*lockdown* | *protected-by* | *restored-from*] [*id*] [**lockdown** | **restored-from**] [*id*] **lockdown**
no path-option [*path id*] {**explicit**} [**name** | **identifier**] [*explicit path name* | *explicit path id*] [**xro-attribute-set**] [*xro attribute set name*] **lockdown verbatim**
no path-option [*path id*] {**dynamic**} [*lockdown* | *protected-by* | *restored-from*] [*restored from id*] [**lockdown** | **restored-from**] [*restored from id*] [**xro-attribute-set**] [*xro attribute set name*] **lockdown**
no path-option [*path id*] **no-ero** [**xro-attribute-set**] [*xro attribute set name*] **lockdown**

Syntax Description

dynamic	Specifies that label switched paths (LSP) are dynamically calculated.
explicit	Specifies that LSP paths are IP explicit paths.
path id	Configures the path option id. The valid range is from 1 to 1000.
path name	Specifies the path name of the IP explicit path.
id	Configures the protected-by id. The valid range is from 1 to 1000.
restored from id	Configures the restored-from id. The valid range is from 1 to 1000.
explicit path name	Configures the explicit path name.
explicit path id	Configures the explicit path id.
xro-attribute-set	Defines the attribute set for circuit diversity.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

At the time of initial setup, if the working LSP does not come-up, GMPLS does not try to bring up service on the restore Path-option; you will need to fix the working path manually.

xro-attribute-set is used only for creating a diverse circuit.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to create a path option for an ODU-Group-Te:

```
RP/0/RP0/CPU0:router(config-mpls-tun-0x7)# path-option 1 explicit name test protected-by 9
 restored-from 8 lockdown
RP/0/RP0/CPU0:router(config-mpls-tun-0x7)# path-option 6 dynamic protected-by 7 restored-from
 8 lockdown
RP/0/RP0/CPU0:router(config-mpls-tun-0x7)# path-option 1 dynamic protected-by none
xro-attribute-set Xro_nni1_tun1_div_tun0 lockdown
RP/0/RP0/CPU0:router(config-mpls-tun-0x7)# no path-option 6 dynamic protected-by 7
restored-from 8 lockdown
```

Example

This example shows how to create a path option for UNI circuits:

```
RP/0/0RP0RSP0/CPU0:router:hostname (config-te-gmpls-cntl)# tunnel-properties path-option 1
 explicit name Exp_path_OPT1_to_OPT5 xro-attribute-set XRO_Tun1_Diverse lockdown verbatim
RP/0/RP0/CPU0:router(config-mpls-tun-0x7)# path-option 1 dynamic protected-by none
xro-attribute-set Xro_nni1_tun1_div_tun0 lockdown
RP/0/0RP0RSP0/CPU0:router:hostname (config-te-gmpls-cntl)# tunnel-properties path-option
10 no-ero lockdown
RP/0/RP0/CPU0:router(config-mpls-tun-0x7)# no path-option 6 dynamic protected-by 7
restored-from 8 lockdown
```

path-protection

To configure the path-protection attribute set, use the **path-protection** command in the config mode. To remove the path-protection attribute set, use the **no** form of this command.

attribute-set {**path-protection-aps**} [*name-of-the-attribute-set*]
gmpls nni {**controller odu-group-te**} *value*
path-protection {**attribute-set**} [*name-of-the-attribute-set*]
no path-protection {**attribute-set**} [*name-of-the-attribute-set*]

Syntax Description

attribute-set	Specifies the attribute-set of the controller.
path-protection-aps	Displays the attribute set of the path protection.
name-of-the-attribute-set	Displays the name of the attribute set.
path-protection	Displays the path protection of the controller.
attribute-set	Displays the path protection attribute set.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Path protection specifies the protection attributes for tunnel.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to configure the static-uni endpoints of the tunnel.

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# attribute-set path-protection-aps ss
RP/0/RP0/CPU0:router(config-te-attribute-set)# exit
RP/0/RP0/CPU0:router(config-mpls-te)# gmpls nni controller odu-group-te 6
RP/0/RP0/CPU0:router(config-te-gmpls-tun-0x6)# path-protection attribute-set ss
```

record-route

To record the route used by a GMPLS OTN tunnel, use the **record-route** command in the config mode. To stop the record-route, use the **no** form of this command.

record-route
no record-route

This command has no keywords or arguments.

Command Default

Disable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Records the route of the GMPLs circuit.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to configure record-route for a GMPLS OTN tunnel.

```
RP/0/RP0/CPU0:router(config-te-gmpls-tun-0x7)# record-route
```

router ID

To configure the ospf router ID, use the **router-id** command in the config mode. To delete the ospf router ID, use the **no** form of this command.

router-id *value*

no router-id *value*

Syntax Description

router-id	Configures the router ID of the OSPF interface.
value	Displays the router ID of the OSPF interface.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the router-ID of the OSPF interface:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# router-id 88.88.88.88
```

router ospf

To configure the router ospf process ID, use the **router ospf** command in the config mode. To delete the router ospf process ID, use the **no** form of this command.

router ospf *process-ID*

no router ospf *process-ID*

Syntax Description

router ospf	Configures the router OSPF process ID.
process-ID	Displays the process ID of the OSPF. Process ID can be numeric, alphanumeric or textual.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the router ospf process-ID:

```
RP/0/RP0:hostname(config)# router ospf 1
```

rsvp controller

To configures RSVP mode of the OTUk controller, use the **rsvp controller** command in the config mode. To delete the RSVP controller, use the **no** form of this command.

rsvp controller {**otuk**} *R/S/I/P*
no rsvp controller {**otuk**} *R/S/I/P*

Syntax Description

rsvp	Enters the controller mode.
otuk	Name of the OTUk controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

RSVP is an external process responsible for signaling the tunnel and maintaining the tunnel states at each node. The TE signal module makes use of the RSVP process, to request the signaling/changing/tearing-down of new LSPs and for handling incoming LSP setup/change/tear-down requests.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to configure RSVP mode of the OTUk controller.

```
RP/0/RP0/CPU0:router(config)# rsvp controller otu2 0/0/0/10
```

record srlg

To record the SRLGs used by a GMPLS UNI connection during signaling, use the **record srlg** command in MPLS-TE GMPLS UNI controller tunnel properties mode. To disable SRLG recording, use the **no** form of this command.

record srlg

no record srlg

Command Default

None

Command Modes

MPLS-TE GMPLS UNI controller tunnel properties configuration.

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
mpls-te	read, write
ouni	read, write

Example

The following example shows how to configure SRLG recording on Optics which is part of GMPLS:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-uni
RP/0/RP0:hostname(config-te-gmpls-uni)# controller optics 0/1/0/2
RP/0/RP0:hostname(config-te-gmpls-uni)# tunnel-properties
RP/0/RP0:hostname(config-te-gmpls-tun)# record srlg
```

show ospf neighbor

To display the odpf ne interface, use the **show ospf neighbor** command in the exec or config mode.

show ospf neighbor

Syntax Description

ospf	Displays the ospf interface.

Command Modes

Exec mode

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

This example shows how to display the ospf on an interface:

```
RP/0/RP0:hostname show ospf neighbor
```

```
Mon Aug 11 03:35:19.672 UTC

* Indicates MADJ interface

Neighbors for OSPF 1

Neighbor ID     Pri   State           Dead Time   Address         Interface
77.77.77.77     1     FULL/  -        00:00:38    8.8.8.2         GCC00/1/0/1
    Neighbor is up for 00:00:06
77.77.77.77     1     FULL/  -        00:00:36    5.5.5.2         GCC00/1/0/12
    Neighbor is up for 00:00:04
```

show mpls traffic-eng tunnels detail

To display the tunnel status and configuration use the **show mpls traffic-eng tunnels detail** command in the exec mode.

show mpls traffic-eng tunnels detail

Syntax Description

mpls	Specifies to display the mpls information.
traffic-eng	Specifies to display traffic engineering information.
tunnels	Specifies to display traffic engineering tunnel status.
detail	Specifies to display extra details of tunnel status and configuration.

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Task ID

Task ID	Operation
otn	read

Example

This example shows how to display details of mpls traffic engineering tunnel status and configuration :

```
RP/0/RP0:hostname # show mpls traffic-eng tunnels detail
```

```
Name: Odu-Group-Te11  Destination: 10.77.132.185  Ifhandle:0x82001e4
  Signalled-Name: 3M_otn11
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 1, (LOCKDOWN) type dynamic  (Basis for Current, path weight 1)
      Protected-by PO index: none
        Reroute pending (DROP)
    Bandwidth Requested: 10037273 kbps  CT0
    Creation Time: Thu Oct  5 08:59:53 2017 (00:45:09 ago)
  Config Parameters:
    Bandwidth: ODU2
    Priority: 24  0 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    Path Selection:
      Tiebreaker: Min-fill (default)
    Hop-limit: disabled
    Cost-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
```

```
    AutoRoute: disabled  LockDown:  enabled  Policy class: not set
    Forward class: 0 (default)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    Soft Preemption: Disabled
  SNMP Index: 72
  Binding SID: None
  Static-uni Info:
    Locally Terminated Interface Name: TenGigE0_1_0_0_200  Ifhandle: 0x82001fc
      Local Termination Type: Ether
      State: Terminated up since Thu Oct  5 08:59:54 2017
      SRLG Values: 2,  7,  8,  20,  21,  33,
  Remote termination Interface: 0.0.0.0 [42]
    Egress Client Port: 0.0.0.0 [42]
  Working Homepath ERO:
    Status: Down
    Explicit Route:
  Diversity Info: None

  History:
    Tunnel has been up for: 00:45:04 (since Thu Oct 05 08:59:58 UTC 2017)
    Current LSP:
      Uptime: 00:45:08 (since Thu Oct 05 08:59:54 UTC 2017)
  Current LSP Info:
    Instance: 302, Signaling Area: OSPF OTN area 0
    Uptime: 00:45:08 (since Thu Oct 05 08:59:54 UTC 2017), Signaling State: Up,
Oper State: Up
    G-PID: Gfp_F Generic Framing Procedure-Framed (54)
      XC Id: 0
      State: Connected
      Uptime: Thu Oct  5 08:59:54 2017
      Egress Interface: OTU40/1/0/0 (State:Up  Ifhandle:0x8a0020c)
      Egress Controller: ODU40_1_0_0 (State:Up Ifhandle:0x8a00214)
      Egress Sub Controller: ODU20_1_0_0_42 (State:Up, Ifhandle:0x82001ec)
      Path Ingress  label: TPN: 4 BitMap Len: 80 BitMap: 25:32
      Resv Egress  label: TPN: 4 BitMap Len: 80 BitMap: 25:32
    Router-IDs: local      10.77.132.187
                downstream 10.77.132.185
    Soft Preemption: None
    SRLGs: mandatory collection
    Path Info:
      Outgoing:
        Explicit Route:
          Strict, 10.77.132.185(19)
          Strict, 10.77.132.185
          Strict, 10.77.132.185(42)

      Record Route: Empty
      Tspec: signal_type ODU2 Bitrate 0kbps NVC 0 MT 1

      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not
Set
                          Soft Preemption Desired: Not Set
    Path Protection Info:
      SNC Mode:SNC-N TCM id:Not used Type:Bi-directional APS
      Path Protection Profile Type: 1+0
      Bits S:0 P:0 N:0 O:0
      Timeout WTR:0 milliseconds HoldOff:0 milliseconds
    Resv Info:
```

```
      Record Route:
        IPv4 10.77.132.185, flags 0x20 (Node-ID)
        Label         Label TPN: 4 BitMap Len: 80 BitMap: 25:32 , flags 0x1

        Unnumbered 10.77.132.185 (19), flags 0x0
        Label         Label TPN: 4 BitMap Len: 80 BitMap: 25:32 , flags 0x1
      Fspec: signal_type ODU2 Bitrate 0kbps NVC 0 MT 1

  Persistent Forwarding Statistics:
    Out Bytes: 0
    Out Packets: 0
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 2 up, 0 down, 0 recovering, 0 recovered heads
```

shutdown lsp-type

To shutdown the Lsp of the tunnel, use the **shutdown lsp-type** command in the config mode. To restart the lsp of the tunnel, use the **no** form of this command.

shutdown
shutdown [**Lsp-type**] [*current* | *restore* | *standby*]
no shutdown [**Lsp-type**] [*current* | *restore* | *standby*]

Syntax Description

shutdown	Shut down the LSP type and tunnel. **Note** If we run the shutdown under odu-group-te, tunnel shuts down .
Lsp type	Specifies the shutdown for particular Lsp type

Command Default

Disable

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If we run the shutdown under odu-group-te, the tunnel shuts down. If you want to shut down that specific LSP then you need to specify the lsp type: working, protected or restore.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to shutdown Lsp-type.

```
RP/0/RP0/CPU0:router(config-te-gmpls-tun-0x7)# shutdown Lsp-type current
```

This example shows to global shutdown.

```
RP/0/RP0/CPU0:router(config-te-gmpls-tun-0x7)# shutdown
```

signalled-bandwidth

To configure the bandwidth required for a GMPLS OTN tunnel, use the **bandwidth command** in the config mode. To delete the bandwidth required for a GMPLS OTN tunnel, use the **no** form of this command.

GFPF is used for Ethernet 10 gig = oduflex 1.25, multiply them by variable.

CBR is used for ODU.

signalled-bandwidth *oduk*
signalled-bandwidth *value***framing type**} [*CBR* | *GFP-F-Fixed*]
no signalled-bandwidth *value***framing type**} [*CBR* | *GFP-F-Fixed*]

Syntax Description

signalled-bandwidth	Specifies the tunnel bandwidth requirement to be signaled. • ODU0: Signalled Bandwidth for ODU0 • ODU1: Signalled Bandwidth for ODU1 • ODU1e: Signalled Bandwidth for ODU • ODU1f: Signalled Bandwidth for ODU1f • ODU2: Signalled Bandwidth for ODU2 • ODU2e: Signalled Bandwidth for ODU2e • ODU2f: Signalled Bandwidth for ODU2f • ODU3: Signalled Bandwidth for ODU3 • ODU3e1: Signalled Bandwidth for ODU3e1 • ODU3e2: Signalled Bandwidth for ODU3e2 • ODU4: Signalled Bandwidth for ODU4 • ODUFlex: Signalled Bandwidth for ODUFlex
ODU2	Configures the odu-type of the ODU group controller.
value	Specifies the tunnel bandwidth range. That is 1 to 104857600 Kbps.
framing type	Specifies the framing type of the controller.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The signaled bandwidth is the ODU signal type that the tunnel uses. In the case of an ODUflex tunnel, the number of 1.25 or 2.5 Gpbs time slots required is automatically computed based on the user provided bit-rate and tolerance.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to configure the bandwidth required for an MPLS-TE tunnel:

```
RP/0/RP0:hostname(config-gmpls-tun-0x7)# signallled-bandwidth odu2 framing-type CBR
RP/0/RP0:hostname(config-gmpls-tun-0x7)# signallled-bandwidth odu2
```

signalled-name

To configure the signal name to the tunnel, use the **signalled-name** command in the config mode. To remove the signal name of the tunnel, use the **no** form of this command.

mpls {**traffic-eng**}
gmpls nni controller {**odu-group-te**} *value*
signalled-name *value*
no signalled-name *value*

Syntax Description

signalled-name	Displays the signal name of the tunnel.
value	Specifies the name of the signal. The maximum length of the signal name is 64 characters.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Signalled name specifies the name of the tunnel.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to configure the static-uni endpoints of the tunnel.

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# gmpls optical-nni
RP/0/RP0/CPU0:router(config-te-gmpls-nni)# controller odu-group-Te 0
RP/0/RP0/CPU0:router(config-te-gmpls-tun-0x0)# signalled-name s1
```

static-uni

To set the static-uni endpoint of the tunnel, use the **static-uni** command in the config mode. To remove the static-uni of the tunnel, use the **no** form of this command.

static-uni {**ingress-port controller**} [*name-of-the-controller R/S/I/P*] {**egress-port unnumbered**} [*value*]
no static-uni {**ingress-port controller**} [*name-of-the-controller R/S/I/P*] {**egress-port unnumbered**} [*value*]

Syntax Description

static-uni	Specifies the static-uni of the tunnel.
ingress-port	Specifies the ingress port.
controller	Specifies the ingress port controller.
name-of-the-controller	Displays the name of the ingress controller.
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
egress-port	Specifies the egress port.
unnumbered	Specifies the tail-end customer port.
value	Enter the tail-end customer port IF index. Use **show snmp interface** command to see the IF index value that starts from 0 to 4294967295. Also, **snmp persist** command to the IF index value static.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The static-uni CLI is used to specify that the NNI tunnel must have its ingress and egress end-points automatically connected to a UNI client port. On the head-end, this cross-connection is done locally. For the tail-end, the cross-connect request is signaled using the RSVP egress control and the tail-end OTN node performs the cross-connect during the tail-end tunnel provisioning.

Task ID

Task ID	Operation
ouni	write

Example

This example shows how to configure the static-uni endpoints of the tunnel.

```
RP/0/RP0/CPU0:router(config-te-gmpls-tun-0x7)# static-uni ingress-port controller otu2
0/0/0/2 egress-port unnumbered 16
```

tunnel-properties

To configure the tunnel properties of a tunnel, use the **tunnel-properties** command in the config mode. To delete the tunnel properties, use the **no** form of this command.

tunnel-properties [**destination** | **logging** | **path-option** | **priority** | **record-route** | **signalled-name** | **tunnel-id**] *value*

no tunnel-properties [**destination** | **logging** | **path-option** | **priority** | **record-route** | **signalled-name** | **tunnel-id**] *value*

Syntax Description

destination	Configures the tunnel destination.
logging	Configures the per-interface logging configuration.
path-option	Configures the GMPLS-UNI path option.
priority	Configures the tunnel priority.
record-route	Record the route used by the tunnel.
signalled-name	Configures the signal name assigned to the tunnel.
tunnel-id	Configures the GMPLS-UNI tunnel ID.
value	Configures the tunnel ID of the tunnel. The valid range of tunnel ID is from 0 to 65535.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to configure the tunnel ID of the tunnel:

```
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-uni controller optics 0/0/0/2
RP/0/RP0:hostname(config-te-gmpls-cntl)# tunnel-properties tunnel-id 55
```

PRBS Command Reference

This chapter describes the commands to configure the PRBS.

controller prbs

To configure prbs controller use the **controller odu opu prbs mode source pattern** command in the config mode.

controller oduk *R/S/I/P* **opu prbs mode** *type* **pattern** *type*

no controller oduk *R/S/I/P* **opu prbs mode** *type* **pattern** *type*]

Syntax Description

controller odu	Name of the controller .
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
opu prbs mode	OPU prbs mode.
pattern	Pattern of the source.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4.6	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
odu	write

Example

The following example shows how to configure prbs.

```
RP/0/RP0:hostnamecontroller odU2 0/15/0/2 opu prbs mode source pattern pn11
```

show controllers

To display all the details of a PRBS, use the **show controllers** command in the exec mode.

show controllers *controller name R/S/I/P* **pm** [**current** | **history**] [**15-min** | **24-hour**] **prbs** *bucket number*

Syntax Description

controller name	Displays the name of the controller.
R/S/I/P	Displays the interface instance of the controller.
pm	Displays the performance monitoring details of the controller.
current	Displays the current values of the controller.
history	Displays the historical values of the controller.
15-min	Configures the 15 minute time interval for the PM parameters.
24-hour	Configures the 24 hour time interval for the PM parameters.
prbs	Configures the prbs.
bucket number	In case of history, it displays the bucket number.

Command Default

None

Command Modes

System Admin EXEC

Command History

Release	Modification
5.2.4.6	This command was introduced

Usage Guidelines

To use these commands in System Admin VM, you must be in a user group associated with appropriate command rules and data rules. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

This example shows how to display the performance parameter of current values tab for 24 hour intervals:

```
RP/0/RP0:hostname # show controllers odu 0/2/0/0 pm current 24-hour prbs
```

This example shows how to display the performance parameter of history values tab for 24 hour intervals:

```
RP/0/RP0:hostname # show controllers odu2 0/4/0/10 pm history 24-hour prbs 1
```

Controllers Breakout Command Reference

This chapter describes the commands to configure controllers breakout.

- Controllers Breakout Command Reference, on page 172
- controller breakout (otn mode), on page 173
- controller breakout (ethernet mode), on page 174
- controller breakout (sonet mode), on page 175
- controller breakout (sdh mode), on page 176
- controller breakout (LAN PHY mode), on page 177
- show breakout-mode, on page 178

Controllers Breakout Command Reference

This chapter describes the commands to configure controllers breakout.

controller breakout (otn mode)

To configure breakout controller in otn mode, use the **controller optics breakout-mode otn** command in the config mode.

controller optics *R/S/I/P* {**breakout-mode** *lane id*} { **otn** }{ **framing** *framing type*}

Syntax Description

controller optics	Name of the controller
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
breakout-mode	Breakout mode.
otn	Type of the controller.
framing	Framing for the breakout-mode.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command contact your AAA administrator for assistance.

Task ID

Task ID	Operation
Breakout	write

Example

The following example shows how to configure a breakout controller:

```
RP/0/RP0:hostname(config)# controller optics 0/15/0/0 breakout-mode 3 otn framing opu2
RP/0/RP0:hostname(config-optics)# commit
```

controller breakout (ethernet mode)

To configure breakout controller in ethernet mode, use the **controller optics breakout-mode ethernet** command in the config mode.

controller optics *R/S/I/P* {**breakout-mode** *lane id*} { **ethernet** } { **framing** *framing type* **mapping** *mapping t ype*}

Syntax Description

controller optics	Name of the controller
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
breakout-mode	Breakout mode.
ethernet	Type of the controller.
framing	Framing for the breakout-mode.
mapping	Mapping for the breakout-mode.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command contact your AAA administrator for assistance.

Task ID

Task ID	Operation
Breakout	write

Example

The following example shows how to configure a breakout controller:

```
RP/0/RP0:hostname(config)# controller optics 0/15/0/0 breakout-mode 3 ethernet framing odu2
 mapping gfpf
RP/0/RP0:hostname(config-optics)# commit
```

controller breakout (sonet mode)

To configure breakout controller in sonet mode, use the **controller optics breakout-mode sonet** command in the config mode.

controller optics *R/S/I/P* {**breakout-mode** *lane id*} { **sonet** } { **framing** *framing type* **mapping** *mapping type*}

Syntax Description

controller optics	Name of the controller
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
breakout-mode	Breakout mode.
sonet	Type of the controller.
framing	Framing for the breakout-mode.
mapping	Mapping for the breakout-mode.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 6.1.2.2	This command was introduced.

Task ID

Task ID	Operation
Breakout	write

Example

The following example shows how to configure a breakout controller:

```
RP/0/RP0:hostname(config)# controller optics 0/11/0/3 breakout-mode 1 sonet framing opu2
mapping bmp
RP/0/RP0:hostname(config-optics)# commit
```

controller breakout (sdh mode)

To configure breakout controller in sdh mode, use the **controller optics breakout-mode sdh** command in the config mode.

controller optics *R/S/I/P* {**breakout-mode** *lane id*} { **sdh** } { **framing** *framing type* **mapping** *mapping type*}

Syntax Description

controller optics	Name of the controller
R/S/I/P	Displays the Rack/Slot/Instance/Port of the controller.
breakout-mode	Breakout mode.
sdh	Type of the controller.
framing	Framing for the breakout-mode.
mapping	Mapping for the breakout-mode.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 6.1.2.2	This command was introduced.

Task ID

Task ID	Operation
Breakout	write

Example

The following example shows how to configure a breakout controller:

```
RP/0/RP0:hostname(config)# controller optics 0/11/0/3 breakout-mode 1 sdh framing opu2
mapping bmp
RP/0/RP0:hostname(config-optics)# commit
```

controller breakout (LAN PHY mode)

To configure breakout controller in LAN PHY mode, use the **controller optics breakout-mode ethernet framing packet** command in the config mode.

controller optics *R/S/I/P* **breakout-mode** *lane id* **ethernet framing** *packet*

Syntax Description

controller optics	Name of the controller
R/S/I/P	Enter the Rack/Slot/Instance/Port of the breakout controller.
breakout-mode	Breakout mode.
ethernet	Type of the controller.
framing *packet*	Set framing type as packet.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 6.1.36	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command contact your AAA administrator for assistance.

Task ID

Task ID	Operation
Breakout	write

Example:

The following example shows how to configure a HundredGigE 0/15/0/0/3 breakout controller in LAN PHY mode:

```
RP/0/RP0:hostname(config)# controller optics 0/15/0/0 breakout-mode 3 ethernet framing
packet
RP/0/RP0:hostname(config-optics)# commit
```

show breakout-mode

To display details of breakout mode, use the **show breakout-mode** command in the exec mode.

show controller optics *R/S/I/P* {**breakout-mode lane** *lane number*} { **capability**}

Syntax Description

optics	Name of the port.
lane number	Displays the Rack/Slot/Instance/Port of the controller.
breakout-mode	Breakout mode.
lane	Displays the lane number.

Command Default

None

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4.6	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command contact your AAA administrator for assistance.

Task ID

Task ID	Operation
Breakout	write

Example

The following example shows how to configure a breakout controller.

```
RP/0/RP0:hostname# show controller optics 0/0/0/1 breakout-mode lane 1 capabilities
```

```
BreakOut Information
------------------------------------------------
Port_no         Breakout Type   Framing                 Mapping
PT type                                         Rate
0               Ethernet        OPU2 framing type       GFP-F mapping type
05 (GFP mapping)                                None
0               Ethernet        OPU2 framing type       GFP-F-Extended mapping
type     09 (GFP mapping into OPU2)                      None
0               Ethernet        OPU Flex framing type   GFP-F mapping type
09 (GFP mapping into OPU2)                      10GE
0               Ethernet        OPU Flex framing type   GFP-F mapping type
09 (GFP mapping into OPU2)                      None
0               OTN             OPU2 framing type       None mapping type
Traffic Dependent                               None
0               OTN             OPU2e framing type      None mapping type
```

```
Traffic Dependent                                   None
0               OTN             OPU1f framing type      None mapping type
Traffic Dependent                                   None
0               OTN             OPU2f framing type      None mapping type
Traffic Dependent                                   None
0               Ethernet        Packet framing type     None mapping type
NA                                                  10GE
RP/0/RP0:SIT06#
```

```
RP/0/RP0:hostname# show controller optics 0/0/0/1 breakout-mode lane 1 configured
```

```
BreakOut Information
-------------------------------------------------
Breakout type   Lane    Framing                 Mapping                 PT type
                                        Rate
Ethernet        1       OPU2 framing type       GFP-F mapping type      05 (GFP
mapping)                                None
RP/0/RP0:SIT06#
```

Patch Cord Command Reference

This chapter describes the commands to configure patch cord between ports.

hw-module patchcord

To configure patch-cord relationship between ports, use the **hw-module patchcord** command in the config mode. The CLI helps the user to tell 'what is connected to what in system'. To delete a patchcord use the no form of this command.

hw-module patchcord port Optics [*R/S/I/P*] **port Optics** [*R/S/I/P*]

no hw-module patchcord port Optics [*R/S/I/P*] **port Optics** [*R/S/I/P*]

Syntax Description

Optics	Name of port
R/S/I/P	Rack/Slot/Instance/Port

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 5.2.4.7	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Two ports should not be same.

None of the ports should be configured on another patchcord.

Duplicate patchcord configuration is not rejected.

Patchcord relationship between ports is bi-directional.

Reverse patchcord configuration of what already exists will be rejected.

Task ID

Task ID	Operation
otn	write

Example

The following example shows how to create a patchcord between two ports:

```
RP/0/RP0:ios(config)#hw-module patchcord port Optics 0/0/0/0 port Optics 0/0/0/1
RP/0/RP0:ios(config)#commit
```

show hw-module patchcord

To show details of a specific patchcord, use the **show hw-module patchcord** command in the exec mode.

To show details of all configured patchcords, use the **show hw-module patchcord all** command in the exec mode.

show hw-module patchcord port Optics [*R/S/I/P*]

show hw-module patchcord all

Syntax Description

Optics	Name of the port.
R/S/I/P	Rack/Slot/Instance/Port of either of the two ports used to configure the patchcord.

Command Default

None

Command Modes

Exec mode

Command History

Release	Modification
Release 5.2.4.7	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
otn	read

Example

The following example shows how to display specific configured patch-chord connectivity.

```
RP/0/0/CPU0:ios # show hw-module patchcord port Optics 0/0/0/0
```

```
Tue Dec 15 11:23:00.945 IST

hw-module patchcord configuration
------------------------------------------------------------------------
Source-Port         Destination-Port
------------------------------------------------------------------------
Optics0_0_0_0       Optics0_0_0_1
```

The following example shows how to display all configured patch-chord connectivity.

```
RP/0/0/CPU0:ios # show hw-module patchcord all
```

```
Tue Dec 15 11:23:00.945 IST

hw-module patchcord configuration
------------------------------------------------------------------------
Source-Port         Destination-Port
------------------------------------------------------------------------
Optics0_0_0_0       Optics0_0_0_1
Optics0_0_0_4       Optics0_0_0_5
Optics0_8_0_0       Optics0_0_5_1
```

Frequency Synchronization Commands

This chapter describes the Cisco IOS XR frequency synchronization commands that are used to distribute precision frequency around a network.

Enabling Frequency Synchronization

To enable Frequency Synchronization globally on the router and to configure Frequency Synchronization options for a controller or interface, use the **frequency synchronization** command in the appropriate configuration mode. To disable Frequency Synchronization, use the **no** form of this command.

frequency synchronization
no frequency synchronization

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Global configuration (config)

Interface configuration (config-interface)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When you configure Frequency Synchronization in global configuration mode, the default clocking is configured for Internal Oscillator. Line timing is used only if Frequency Synchronization is enabled on Line interfaces.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to enable Frequency Synchronization in global configuration:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# frequency synchronization
RP/0/RP0:hostname(config-freqsync)# commit
```

The following example shows how to enable Frequency Synchronization on an Ethernet interface:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface tenGigE 0/5/0/0
RP/0/RP0:hostname(config-if)# frequency synchronization
RP/0/RP0:hostname(config-if-freqsync)# commit
```

clear Frequency Synchronization esmc statistics

To clear the Ethernet Synchronization Messaging Channel (ESMC) statistics, use the **clear frequency synchronization esmc statistics** command in EXEC mode.

clear frequency synchronization esmc statistics interface {*interface* | **all** | **summary** **location** {*node-id* | **all**}}

Syntax Description

interface	The command can be restricted to clear the ESMC statistics for a particular interface by specifying the interface.
node-id	The output can be restricted to clear the ESMC statistics for a particular node by specifying the location. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear the ESMC statistics on specific interface: :

```
RP/0/RP0:hostname# clear frequency synchronization esmc statistics interface tenGigE0/1/0/1
```

clear Frequency Synchronization wait-to-restore

To clear the Frequency Synchronization wait-to-restore timer, use the **clear frequency synchronization wait-to-restore** command in EXEC mode.

clear frequency synchronization wait-to-restore {**all** | {**frequency synchronization** *port-num* **location** *node-id*} | **interface** {*type interface-path-id* | **all**}}

Syntax Description

all	Clears all wait-to-restore timers.
interface *type interface-path-id*	Clears the wait-to-restore timers for a specific interface or all interfaces.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear the Frequency Synchronization wait-to-restore timer on specific interface:

```
RP/0/RP0:ios# clear frequency synchronization wait-to-restore interface tenGigE0/1/0/1
```

log selection

To enable logging of changes or errors to Frequency Synchronization, use the **log selection** command in Frequency Synchronization configuration mode. To disable logging, use the **no** form of this command.

log selection {**changes** | **errors**}
no log selection

Syntax Description

changes	Logs every time there is a change to the selected source, including any logs that the **errors** keyword logs.
errors	Logs only when there are no available frequency sources, or when the only available frequency source is the internal oscillator.

Command Default

No default behavior or values

Command Modes

Frequency Synchronization configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

This example shows how to enable logging of changes to Frequency Synchronization:

```
RP/0/RP0:ios(config)# config
RP/0/RP0:ios(config)# frequency synchronization
RP/0/RP0:ios(config-freqsync)# log selection changes
RP/0/RP0:ios(config-freqsync)# commit
```

priority (Frequency Synchronization)

To configure the priority of the frequency source on an interface, use the **priority** command in the Interface Frequency Synchronization configuration mode. To return the priority to the default value, use the no form of this command.

priority *priority-value*
no priority *priority-value*

Syntax Description

priority-value	Priority of the frequency source. The priority is used to select between sources with the same Quality Level (QL). The range is 1 (highest priority) to 254 (lowest priority).

Command Default

100

Command Modes

Interface Frequency Synchronization configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to configure the Frequency Synchronization priority on an interface:

```
RP/0/RP0:ios(config)# config
RP/0/RP0:ios(config)# interface tenGigE 0/1/0/1
RP/0/RP0:ios(config-if)# frequency synchronization
RP/0/RP0:ios(config-if-freqsync)# priority 150
RP/0/RP0:ios(config-if-freqsync)# commit
```

quality itu-t option

To configure the quality level (QL) options, use the **quality itu-t option** command in Frequency Synchronization configuration mode. To return to the default levels, use the **no** form of this command.

quality itu-t option {**1** | **2 generation** {**1** | **2**}}
no quality

Syntax Description

{**1** | **2 generation** {**1** | **2**}} Specifies the quality level for the router. Valid options are:

- **1**—ITU-T QL option 1, which uses the PRC, SSU-A, SSU-B, SEC and DNU quality levels.
- **2 generation 1**—ITU-T QL option 2 generation 1, which uses the PRS, STU, ST2, ST3, SMC, ST4, RES and DUS quality levels.
- **2 generation 2**—ITU-T QL option 2, generation 2, which uses the PRS, STU, ST2, ST3 TNC, ST3E, SMC, ST4, PROV and DUS quality levels.

Command Default

ITU-T option 1

Command Modes

Frequency Synchronization configuration

Note The QL should match with what is configured in global option.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The QL configured with the **quality itu-t option** command must match the QL specified in the **quality transmit** and **quality receive** commands configured in interface Frequency Synchronization configuration mode.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to configure the ITU-T QL options:

```
RP/0/RP0:ios#config
RP/0/RP0:ios(config)# frequency synchronization
RP/0/RP0:ios(config-freqsync)# quality itu-t option 1
RP/0/RP0:ios(config-freqsync)# commit
```

quality receive

To configure all the Synchronization Status Message (SSM) quality levels (QLs) for the frequency source from the receive interface, use the **quality receive** command in the appropriate Frequency Synchronization mode. To return to the default levels, use the no form of this command.

quality receive itu-t option { **lowest** *ql-option ql* [**highest** *ql*] | **highest** *ql-option ql* | **exact** *ql-option ql* }
no quality receive

Syntax Description

ql-option Quality Level (QL) options.

Valid values are:

- **1**—ITU-T Option 1
- **2 generation 1**—ITU-T Option 2 Generation 1
- **2 generation 2**—ITU-T Option 2 Generation 2

ql Quality Level (QL) value.

For line interfaces and clock interface with SSM support, any of the following combinations of QL values can be specified to modify the QL value received via SSM:

- If the **exact** keyword is used and the received or default QL is not DNU, then this value is used (rather than the received/default QL).
- If the **lowest** keyword is used and the received QL is a lower quality than this, then the received QL value is ignored and DNU is used instead.
- If the **highest** keyword is used and the received QL is higher quality than this, then the received QL value is ignored and this value is used instead.
- If the **lowest** and **highest** keywords are used, the behavior is as above. The maximum QL must be at least as high quality as the minimum QL.

Valid QL values for ITU-T Option 1 are:

- PRC
- SSU-A
- SSU-B
- SEC
- DNU

Valid QL values for ITU-T Option 2 Generation 1 are:

- PRS
- STU
- ST2
- ST3
- SMC
- ST4
- RES
- DUS

Valid QL values for ITU-T Option 2 Generation 2 are:

- PRS
- STU
- ST2
- TNC
- ST3E
- ST3
- SMC
- ST4
- PROV
- DUS

Command Default

QL is unmodified.

Command Modes

Interface Frequency Synchronization

Note Quality configuration should match with what is configured in global option.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

In cases where the clock interface supports SSM but it is not always enabled, all options are available.

Note If SSM is disabled, only the exact QL option is available.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following examples shows how to configure all the SSM quality levels for the frequency source from the receive interface:

```
RP/0/RP0:ios# config
RP/0/RP0:ios(config)# int tenGigE0/2/0/7
RP/0/RP0:ios(config-if)# frequency synchronization
RP/0/RP0:ios(config-if-freqsync)# quality receive exact itu-t option 1 PRC
RP/0/RP0:ios(config-if-freqsync)# commit


RP/0/RP0:ios# config
RP/0/RP0:ios(config)# clock-interface Rack0-Bits0-In
```

```
RP/0/RP0:ios(config-clock-if)# port-parameters etsi bits-input e1 fas ami
RP/0/RP0:ios(config-clock-if)# frequency synchronization
RP/0/RP0:ios(config-clk-freqsync)# selection input
RP/0/RP0:ios(config-clk-freqsync)# wait-to-restore 0
RP/0/RP0:ios(config-clk-freqsync)# quality receive highest itu-t option 1 PRC
RP/0/RP0:ios(config-clk-freqsync)# commit
```

quality transmit

To configure all the Synchronization Status Message (SSM) quality levels for the frequency source from the transmit interface, use the **quality transmit** command in the appropriate Frequency Synchronization mode. To return to the default levels, use the **no** form of this command.

quality transmit itu-t option { **lowest** *ql-option ql* [**highest** *ql*] | **highest** *ql-option ql* | **exact** *ql-option ql* }
no quality transmit

Syntax Description

ql-option Quality Level (QL) ITU-T options.

Valid values are:

- **1**—ITU-T Option 1
- **2 generation 1**—ITU-T Option 2 Generation 1
- **2 generation 2**—ITU-T Option 2 Generation 2

ql Quality Level (QL) value.

For line interfaces with SSM support, any of the following combinations of QL values can be specified to modify the QL value received via SSM:

- If the **exact** keyword is used and the received or default QL is not DNU, then this value is used (rather than the received/default QL).
- If the **lowest** keyword is used and the received QL is a lower quality than this, then the received QL value is ignored and DNU is used instead.
- If the **highest** keyword is used and the received QL is higher quality than this, then the received QL value is ignored and this value is used instead.
- If the **lowest** and **highest** keywords are used, the behavior is as above. The maximum QL must be at least as high quality as the minimum QL.

Valid QL values for ITU-T Option 1 are:

- PRC
- SSU-A
- SSU-B
- SEC
- DNU

Valid QL values for ITU-T Option 2 Generation 1 are:

- PRS
- STU
- ST2
- ST3
- SMC
- ST4
- RES
- DUS

Valid QL values for ITU-T Option 2 Generation 2 are:

- PRS
- STU
- ST2
- TNC
- ST3E
- ST3
- SMC
- ST4
- PROV
- DUS

Command Default

The QL is unmodified

Command Modes

Interface Frequency Synchronization

Note Quality configuration should match with what is configured in global option.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If the interface is the selected source, DNU is always sent regardless of this configuration.

This configuration has no effect when SSM is disabled.

Note For clock interfaces that do not support SSM, only the lowest QL can be specified. In this case, rather than sending DNU, the output is squelched, and no signal is sent.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following examples show how to configure all the SSM quality levels for the frequency source from the transmit interface:

```
RP/0/RP0:ios# config
RP/0/RP0:ios(config)# int tenGigE0/2/0/7
RP/0/RP0:ios(config-if)# frequency synchronization
RP/0/RP0:ios(config-if-freqsync)# quality transmit exact itu-t option 2 generation 1 PRS
RP/0/RP0:ios(config-if-freqsync)# commit
```

```
RP/0/RP0:ios# config
RP/0/RP0:ios(config)# clock-interface Rack0-Bits0-Out
RP/0/RP0:ios(config-clock-if)# port-parameters etsi bits-input e1 fas ami
RP/0/RP0:ios(config-clock-if)# frequency synchronization
RP/0/RP0:ios(config-clk-freqsync)# quality transmit highest itu-t option 1 PRC
RP/0/RP0:ios(config-clk-freqsync)# commit
```

selection input

To configure an interface so that it is available as a timing source for selection by the system, use the **selection input** command in the appropriate Frequency Synchronization configuration mode. To remove the interface as an available timing source, use the **no** form of this command.

Note At a time, only two configured line interfaces participate in frequency synchronization.

selection input
no selection input

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface Frequency Synchronization configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to configure an interface so that it is available as a timing source for selection by the system:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface tenGigE0/1/0/1
RP/0/RP0:hostname(config-if)# frequency synchronization
RP/0/RP0:hostname(config-if-freqsync)# selection input
RP/0/RP0:hostname(config-if-freqsync)# commit
```

clock-interface

To configure a clock controller, use the **clock-interface** command in the config mode. To delete the controller, use the no form of this command.

clock-interface [**Rack0-Bits0-In** | **Rack0-Bits0-Out** | **Rack0-Bits1-In** | **Rack0-Bits1-Out**]
port-parameters [**Interface Type**] [**bits-input** | **bits-output**] [**BITS mode**]

Following are valid port-parameter commands:

port-parameters [**ansi** | **etsi**] **bit-input 64k**
port-parametersetsi [**bit-input** | **bit-output**] **2m**
port-parametersetsi [**bit-input** | **bit-output**] **e1 crc-4** [**sa4** | **sa5** | **sa6** | **sa7** | **sa8**] [**ami** | **hdb3**]
port-parametersetsi [**bit-input** | **bit-output**] **e1 fas** [**ami** | **hdb3**]
port-parametersansi bit-output j1 [**d4** | **esf**] [**ami** | **b8zs**]
port-parametersansi bit-input [**j1** | **t1**] [**d4** | **esf**] [**ami** | **b8zs**]
port-parametersansi bit-output t1 [**d4** | **esf**] [**ami** | **b8zs**] [**0** | **1** | **2** | **3** | **4**]
no port-parameters

Syntax Description

Interface Type	Type of clock interface. Valid values are ANSI and ETSI.
BITS mode	BITS mode.

Command Default

None.

Command Modes

Config mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Examples

The following example shows how to configure a clock interface:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# clock-interface Rack0-Bits0-Out
RP/0/RP0:hostname(config-Optics)# port-parameters etsi bits-output e1 crc-4 sa4 ami
RP/0/RP0:hostname(config-Optics)# commit
```

show Frequency Synchronization configuration-errors

To display information about any configuration inconsistencies that are detected, but that are not rejected by verification, use the **show frequency synchronization configuration-errors** command in EXEC mode.

show frequency synchronization configuration-errors [**location** *node-id*]

Syntax Description

location	Location of the card, specified by *node-id*.
node-id	The output can be restricted to a particular node by specifying the location. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

This example shows the normal output for the **show frequency synchronization configuration-errors** command:

```
RP/0/RP0:hostname # show frequency synchronization configuration-errors

Thu Jan 19 09:55:42.779 UTC
Node 0/RP0:
==============
interface TenGigE0/13/0/7 frequency synchronization quality
transmit exact itu-t option 2 generation 1 PRS
* The QL that is configured is from a different QL option set than is configured globally.
```

show frequency synchronization interfaces

To show the Frequency Synchronization information for all interfaces or for a specific interface, use the **show frequency synchronization interfaces** command in EXEC mode.

show frequency synchronization interfaces {**brief** | **summary** [**location** *node-id*] | *type interface-path-id*}

Syntax Description

brief	Displays brief information for all interfaces.
summary [**location** *node-id*]	Displays summary information for all notes or a specific node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.
type interface-path-id	Displays information for a specific interface.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows the display output for the **show frequency synchronization interfaces** command:

```
RP/0/RP0:hostname#show frequency synchronization interfaces
Interface FortyGigE0/7/0/2 (unknown)
  Wait-to-restore time 0 minutes
  SSM Enabled
  Input:
    Down - not assigned for selection
    Supports frequency
  Output:
    Selected source: None
    Effective QL: DNU
  Next selection points: LC7_ING_SEL
```

The output in brief mode is as follows:

```
RP/0/RP0:hostname#show frequency synchronization interfaces brief

Flags:  > - Up               D - Down             S - Assigned for selection
        d - SSM Disabled     x - Peer timed out   i - Init state
        s - Output squelched
Fl   Interface                QLrcv QLuse Pri QLsnd Output driven by
==== ======================== ===== ===== === ===== ========================
```

```
>S   TenGigE0/2/0/7           ST3   ST3   100 PRS   TenGigE0/13/0/7
>S   TenGigE0/2/0/8           ST3   ST3   100 PRS   TenGigE0/13/0/7
>    TenGigE0/13/0/5          PRS   Fail  100 PRS   TenGigE0/13/0/7
>    TenGigE0/13/0/6          PRS   Fail  100 PRS   TenGigE0/13/0/7
>S   TenGigE0/13/0/7          PRS   PRS   100 DUS   TenGigE0/13/0/7
>S   TenGigE0/13/0/8          ST3   ST3   100 PRS   TenGigE0/13/0/7
D    HundredGigE0/13/0/0      Fail  Fail  100 PRS   TenGigE0/13/0/7
```

The output in summary mode is as follows, for each node:

```
RP/0/RP0:hostname#show frequency synchronization summary

1 Ethernet interfaces in Synchronous mode, 0 assigned for selection, 1 with SSM enabled

    ESMC SSMs        Total  Information     Event    DNU/DUS
      Sent:          23236        23168        68        200
      Received:      23164        23162         2      19364
```

show frequency synchronization clock-interfaces

To display the frequency synchronization information for all clock-interfaces or for a specific node, use the **show frequency synchronization clock-interfaces** command in EXEC mode.

show frequency synchronization clock-interface [**brief**] [**location** *node-id*]

Syntax Description

brief	Displays summary information for all clock interfaces.
location *node-id*	(Optional) Displays information for a specific interface. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute
sonet-sdh	execute

Examples

The following example shows the display output for the **show frequency synchronization clock-interfaces** command:

```
RP/0/RP0:hostname#show frequency synchronization clock-interfaces

Node 0/RP0:
==============
Clock interface Sync0 (Down: NONE)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input:
      Down - not assigned for selection
      Last received QL: None
      Supports frequency
    Output is disabled
  Next selection points: T0_SEL

  Clock interface Sync1 (Down: NONE)
    Wait-to-restore time 0 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: None
      Effective QL: DNU
  Next selection points: None
```

```
  Clock interface Sync2 (Down: NONE)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input:
      Down - not assigned for selection
      Last received QL: None
      Supports frequency
    Output is disabled
  Next selection points: T0_SEL

  Clock interface Sync3 (Down: NONE)
    Wait-to-restore time 0 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: None
      Effective QL: DNU
  Next selection points: None

  Clock interface Internal0 (Up)
    Assigned as input for selection
    Input:
      Default QL: None
      Effective QL: Failed, Priority: 255, Time-of-day Priority 255
      Supports frequency
  Next selection points: T0_SEL T4_SEL
```

The output in brief mode is as follows:

```
RP/0/RP0:hostname#show frequency synchronization clock-interfaces brief

Flags:  > - Up                D - Down              S - Assigned for selection
        d - SSM Disabled      s - Output squelched  L - Looped back
Node 0/RP0:
==============
  Fl    Clock Interface     QLrcv  QLuse  Pri QLsnd  Output driven by
  ===== ================== ====== ====== === ====== ========================
  D     Sync0               None   Fail   100 n/a    n/a
  D     Sync1               n/a    n/a    n/a DNU    None
  D     Sync2               None   Fail   100 n/a    n/a
  D     Sync3               n/a    n/a    n/a DNU    None
  DS    Internal0           n/a    Fail   255 n/a    n/a
```

The output for particular location is as follows:

```
RP/0/RP0:hostname#show frequency synchronization clock-interfaces location 0/RP0

Node 0/RP0:
==============
  Clock interface Sync0 (Unknown state)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input:
      Down - not assigned for selection
      Last received QL: None
      Supports frequency
    Output is disabled
  Next selection points: T0_SEL

  Clock interface Sync1 (Unknown state)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
```

```
  Input is disabled
  Output:
    Selected source: None
    Effective QL: DNU
Next selection points: None

Clock interface Sync2 (Unknown state)
  Wait-to-restore time 5 minutes
  SSM supported and enabled
  Input:
    Down - not assigned for selection
    Last received QL: None
    Supports frequency
  Output is disabled
Next selection points: T0_SEL

Clock interface Sync3 (Unknown state)
  Wait-to-restore time 5 minutes
  SSM supported and enabled
  Input is disabled
  Output:
    Selected source: None
    Effective QL: DNU
Next selection points: None

Clock interface Internal0 (Unknown state)
  Assigned as input for selection
  Input:
    Default QL: None
    Effective QL: Failed, Priority: 255, Time-of-day Priority 255
    Supports frequency
Next selection points: T0_SEL T4_SEL
```

show controllers slice-control all location

To display the clock source information for the LC, use the **show controllers slice-control all location** command in EXEC mode.

show controllers slice-control all location <*LC location*>

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.2.4	This command was introduced.

Examples

The following example shows the display output for the **show controllers slice-control all location** command:

```
RP/2/RP0:MC_FLT+4+1# show controllers slice-control all location 0/LC1
Thu Mar 22 14:36:42.685 IST
CARD 0 IS OFFLINE
CARD 1 IS OFFLINE
CARD 3 IS OFFLINE
CARD 8 IS OFFLINE
CARD 10 IS OFFLINE
CARD 11 IS OFFLINE
CARD 12 IS OFFLINE
CARD 13 IS OFFLINE
CARD 14 IS OFFLINE
=============================================
Slice Controller Context: 2
=============================================
Inserted              : Yes
Physical Slot number  : 3
Logical slot number   : 2
Board type            : 5408a5 (BOARD_TYPE_SCAPA_1x100GE_CPAK_10x10GE)
Slice oper state      : OPERATIONAL
Bao Version           : 0.1.59
Hotplug status        : ONLINE
PCI Bar Address       : 0xb064000000
MSI                   : c9
PLLs locked           : Yes
PLLs Init Status      : PLL Initialized
PLLs Reset Status     : PLL Reset Skipped
Clock Status          : External (RP0)
Hardware ID           : |e08:3_e_2.0
```

show controllers timing controller

To display the summary of the timing controller configuration, use the **show controllers timing controller { clock | te-port}** command in EXEC mode.

show controllers timing controller clock
show controllers timing controller te-port

Syntax Description

clock	Displays the clock interface settings.
te-port	Displays the te interface settings.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.25	This command was updated for Multi Chassis.
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows the display output for the **show controllers timing controller clock** command:

```
RP/0/RP0:hostname#show controllers timing controller clock

SYNCEC Clock-Setting:

          Port 0          Port 1          Port 2          Port 3
Config     : No             Yes             No             Yes
BITS Mode  : -              E1              -              E1
Framing    : -              CRC4            -              CRC4
Linecoding : -              AMI             -              AMI
Submode    : -              Sa4             -              Sa4
Shutdown   : No             No              No             No
Direction  : RX             TX              RX             TX
QL Option  : O1             O1              O1             O1
RX_ssm     : -              -               -              -
TX_ssm     : -              SEC             -              SEC
If_state   : ADMIN_DOWN     DOWN            ADMIN_DOWN     DOWN
```

Examples

The following example shows the display output for the **show controllers timing controller te-port** command:

```
RP/2/RP0:MC_FLT+4+1# show controllers timing controller te-port
Thu Mar 22 11:43:01.307 IST

FSYNCDIR TE-Port Setting: Rack 0

FSYNC Mastership Rack 0: MASTER
          TE0-E           TE1-E           TE0-W           TE1-W
TE state : FORWARDING     FORWARDING      FORWARDING      FORWARDING
Rx Signal: No             No              No              No
Link     : Good           Good            Good            Good
PeerRack : 1              1               3               3
PeerPort : TE0-W          TE1-W           TE0-E           TE1-E
DELAY(ns): 240            240             235             240


FSYNCDIR TE-Port Setting: Rack 1

FSYNC Mastership Rack 1: SLAVE
          TE0-E           TE1-E           TE0-W           TE1-W
TE state : FORWARDING     FORWARDING      MASTER          BACKUP
Rx Signal: No             No              Yes             Yes
Link     : Good           Good            Good            Good
PeerRack : 2              2               0               0
PeerPort : TE0-W          TE1-W           TE0-E           TE1-E
DELAY(ns): 235            240             240             240


FSYNCDIR TE-Port Setting: Rack 2

FSYNC Mastership Rack 2: SLAVE
          TE0-E           TE1-E           TE0-W           TE1-W
TE state : ALTERNATE      ALTERNATE       MASTER          BACKUP
Rx Signal: Yes            Yes             Yes             Yes
Link     : Good           Good            Good            Good
PeerRack : 3              3               1               1
PeerPort : TE0-W          TE1-W           TE0-E           TE1-E
DELAY(ns): 240            235             240             240


FSYNCDIR TE-Port Setting: Rack 3

FSYNC Mastership Rack 3: SLAVE
          TE0-E           TE1-E           TE0-W           TE1-W
TE state : MASTER         BACKUP          ALTERNATE       ALTERNATE
Rx Signal: Yes            Yes             Yes             Yes
Link     : Good           Good            Good            Good
PeerRack : 0              0               2               2
PeerPort : TE0-W          TE1-W           TE0-E           TE1-E
DELAY(ns): 235            240             240             235
```

show frequency synchronization interfaces brief

To display frequency synchronization interface details, use the **show frequency synchronization interfaces brief** command in the appropriate mode.

show frequency synchronization interfaces brief

Syntax Description

brief	Displays the brief interface information.

Command Default

No default behavior or values

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

None

Example

This example shows how to use the **show frequency synchronization interfaces brief** command:

```
RP/0/RP0:MC_OTN#show frequency synchronization interfaces brief

Thu Mar 22 14:42:52.032 IST
Flags:  > - Up                D - Down              S - Assigned for selection
        d - SSM Disabled      x - Peer timed out    i - Init state
        s - Output squelched
Fl   Interface                QLrcv QLuse Pri QLsnd Output driven by
==== ======================== ===== ===== === ===== ========================
>    TenGigE0/9/0/2           DNU   n/a   100 PRC   Rack2-Bits0-In
>S   TenGigE0/9/0/8           PRC   PRC   200 PRC   Rack2-Bits0-In
>S   TenGigE2/4/0/2           SSU-A SSU-A 100 PRC   Rack2-Bits0-In
>S   FortyGigE2/15/0/6        PRC   PRC    10 PRC   Rack2-Bits0-In
```

show Frequency Synchronization selection

To display the Frequency Synchronization selection information for all selection points or for a specific node, use the **show frequency synchronization selection** command in EXEC mode.

show frequency synchronization selection {**location** *node-id*}

Syntax Description

location *node-id*	Displays information for a specific node on the router. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **show frequency synchronization selection** command shows the status of the timing stream from the timing source

Task ID

Task ID	Operations
ethernet-services	execute

Examples

This example shows the normal output for the **show frequency synchronization selection** command:

```
RP/0/RP0:ios # show frequency synchronization selection

Node 0/RP0:
==============
Selection point: T0_SEL (4 inputs, 1 selected)
  Last programmed 00:05:34 ago, and selection made 00:05:18 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T4_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  Used for local line interface output
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  1  Sync2 [0/RP0]             n/a                        PRS   99  Locked
     TenGigE0/7/0/9/4          0/RP0 LC7_ING_SEL 1        PRS  100  Available
     TenGigE0/13/0/0/6         0/RP0 LC13_ING_SEL 1       STU  100  Available
     Internal0 [0/RP0]         n/a                        ST3  255  Available

Selection point: T4_SEL (2 inputs, 1 selected)
  Last programmed 00:05:22 ago, and selection made 00:05:18 ago
  Next selection points
    SPA scoped    : None
```

```
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  Used for local clock interface output
  S  Input                      Last Selection Point          QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  1  Sync2 [0/RP0]              0/RP0 T0_SEL 1              PRS   99  Locked
     Internal0 [0/RP0]          n/a                         ST3  255  Available

Selection point: LC0_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC1_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC2_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC3_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC4_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC5_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
```

```
Selection point: LC6_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC7_ING_SEL (1 inputs, 1 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:35 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  1  TenGigE0/7/0/9/4          n/a                         PRS  100  Available

Selection point: LC8_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC9_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC10_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC11_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC12_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
```

```
  Uses frequency selection

Selection point: LC13_ING_SEL (2 inputs, 1 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:34 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point          QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  1  TenGigE0/13/0/0/6         n/a                         STU  100  Available
     TenGigE0/13/0/8           n/a                         STU  100  Available

Selection point: LC14_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection

Selection point: LC15_ING_SEL (0 inputs, 0 selected)
  Last programmed 00:05:36 ago, and selection made 00:05:36 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
```

show Frequency Synchronization selection back-trace

To display the path that was followed by the clock source that is being used to drive a particular interface use the **show frequency synchronization selection back-trace** command in EXEC mode.

show frequency synchronization selection back-trace {*port-num* | **interface** *type interface-path-id* | *node-id*}

Syntax Description

interface *type interface-path-id*	Displays the path to the specified interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **show frequency synchronization selection back-trace** command displays the trace from the specified target interface, back to the clock source being used to drive it. The display includes the selection points that are being hit along the way.

Task ID

Task ID	Operation
ethernet-services	read

This example shows sample output from the **show frequency synchronization selection back-trace** command:

```
RP/0/RP0:ios# show frequency synchronization selection back-trace interface TenGigE0/7/0/9/1
Selected Source: TenGigE0/7/0/9/1
Selection Points:
  0/RP0 T0_SEL
  0/RP0 LC7_ING_SEL
```

show Frequency Synchronization selection forward-trace

To display the path that was recovered from a particular interface, use the **show frequency synchronization selection forward-trace**

show frequency synchronization selection forward-trace {*port-nu* | **interface** *type interface-path-id* | *node-id*}

Syntax Description

interface *type interface-path-id*	Displays the path to the specified interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **show frequency synchronization selection forward-trace** command displays the trace from the specified interface, out to all selection points that receive the clock from the interface, and from any interfaces that are potentially being driven by this clock source.

Task ID

Task ID	Operation
ethernet-services	read

This example shows sample output from the **show frequency synchronization selection forward-trace** command:

```
RP/0/RP0:ios#show frequency synchronization selection forward-trace interface TenGigE0/7/0/9/1
0/RP0 LC7_ING_SEL
0/RP0 T0_SEL
0/RP0 T4_SEL
 Sync0 [0/RP0]
 Sync1 [0/RP0]
 Sync2 [0/RP0]
 Sync3 [0/RP0]

TenGigE0/10/0/9/
TenGigE0/7/0/9/1
```

show running-config frequency synchronization

To display the current operating configuration information for frequency synchronization, use the **show running-config frequency synchronization** command in EXEC mode.

show running-config frequency synchronization

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Examples

The following example shows the display output for the **show running-config frequency synchronization** command:

```
RP/2/RP0:MC_FLT+4+1# show running-config frequency synchronization
Thu Mar 22 11:33:30.986 IST
frequency synchronization
clock-interface timing-mode system
```

ssm disable

To disable Synchronization Status Messaging (SSM) on an interface, use the **ssm disable** command in the appropriate Frequency Synchronization configuration mode. To return SSM to the default value of enabled, use the **no** form of this command.

ssm disable
no ssm disable

Command Default

Enabled

Command Modes

Interface Frequency Synchronization configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

For Frequency Synchronization interfaces, the **ssm disable** command disables sending ESMC packets, and ignores any received ESMC packets.

The received QL value that is used if SSM is disabled depends on the option:

- Option 1: DNU
- Option 2: STU

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to disable SSM on an interface:

```
RP/0/RP0:ios # config
RP/0/RP0:ios(config)# interface tenGigE 0/1/0/1
RP/0/RP0:ios(config-if)# frequency synchronization
RP/0/RP0:ios(config-if-freqsync)# ssm disable
RP/0/RP0:ios(config-if-freqsync)# commit
```

wait-to-restore

To configure the wait-to-restore time for Frequency Synchronization on an interface, use the **wait-to-restore** command in the appropriate Frequency Synchronization configuration mode. To return the wait-to-restore time to the default value, use the **no** form of this command.

wait-to-restore *minutes*
no wait-to-restore *minutes*

Syntax Description

minutes	The delay time (in minutes) between when an interface comes up and when it is used for synchronization. The range is 0 to 12.

Command Default

There is a 5-minute delay for Frequency Synchronization after an interface comes up.

Command Modes

Interface Frequency Synchronization (config-if-freqsync)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to configure the wait-to-restore time for Frequency Synchronization on an interface:

```
RP/0/RP0:ios # config
RP/0/RP0:ios(config)# interface tenGigE0/1/0/1
RP/0/RP0:ios(config-if)# frequency synchronization
RP/0/RP0:ios(config-if-freqsync)# wait-to-restore 0
RP/0/RP0:ios(config-if-freqsync)# commit
```

IPv4/OSPF Commands

This chapter describes the commands used to configure and monitor the Open Shortest Path First (OSPF) routing protocol.

address-family (OSPF)

To enter address family configuration mode for Open Shortest Path First (OSPF), use the **address-family** command in the appropriate mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv4 [**unicast**]
no address-family ipv4 [**unicast**]

Syntax Description

ipv4	Specifies IP Version 4 (IPv4) address prefixes.
unicast	(Optional) Specifies unicast address prefixes.

Command Default

An address family is not specified.

Command Modes

Router configuration

VRF Configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

OSPF version 2 automatically provides routing services for IPv4 unicast topologies, so this command is redundant.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the OSPF router process with IPv4 unicast address prefixes:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# address-family ipv4 unicast
```

adjacency stagger

To configure staggering of OSPF adjacency during reload, process restart, and process clear, use the **adjacency stagger** command in router configuration mode. To turn off adjacency staggering, either use the **disable** keyword or use the **no** form of this command.

adjacency stagger {**disable** | *initial-num-nbr* *max-num-nbr*}
no adjacency stagger

Syntax Description

disable	Disables adjacency staggering.
initial-num-nbr	The initial number of simultaneous neighbors allowed to form adjacency to FULL in any area to bring up to FULL after a router reload, OSPF process restart, or OSPF process clear. Range is 1-65535. Default is 2.
max-num-nbr	The subsequent number of simultaneous neighbors allowed to form adjacency, per OSPF instance, after the initial set of OSPF neighbors have become FULL. Range is 1-65535. Default is 64.

Command Default

OSPF adjacency staggering is enabled.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Staggering of the OSPF adjacency during reload, process restart (without NSR or graceful-restart), and process clear reduces the overall adjacency convergence time.

Initially, allow 2 (configurable) neighbors to form adjacency to FULL per area. After the first adjacency reaches FULL, up to 64 (configurable) neighbors can form adjacency simultaneously for the OSPF instance (all areas). However, areas without any FULL adjacency is restricted by the initial area limit.

Note Adjacency stagger and OSPF nonstop forwarding (NSF) are mutually exclusive. Adjacency stagger will not be activated if **nsf** is configured under router ospf configuration.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure adjacency stagger for a 2 neighbors initially and for a maximum of 3 neighbors:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# adjacency stagger 2 3
```

area (OSPF)

To configure an Open Shortest Path First (OSPF) area, use the **area** command in the appropriate mode. To terminate an OSPF area, use the **no** form of this command.

area *area-id*
no area *area-id*

Syntax Description

area-id	Identifier of an OSPF area. The *area-id* argument can be specified as either a decimal value or an IP address (dotted decimal) format. Range is 0 to 4294967295.

Command Default

No OSPF area is defined.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **area** command to explicitly configure an area. Commands configured under the area configuration mode (such as the **interface** [OSPF] and **authentication** commands), are automatically bound to that area.

To modify or remove the area, the *area-id* argument format must be the same as the format used when creating the area. Otherwise, even if the actual 32-bit value matches, the area is not matched. For example, if you create an area with an *area-id* of 10 it would not match an *area-id* of 0.0.0.10.

Note To remove the specified area from the router configuration, use the **no area** *area-id* command. The **no area** *area-id* command removes the area and all area options, such as **authentication** , **default-cost** , **nssa** , **range** , **stub** , **virtual-link** , and **interface.**

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure area 0 and Ten Gigabit Ethernet interface 0/6/0/2.10. Ten Gigabit Ethernet interface 0/6/0/2.10 is bound to area 0 automatically.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

authentication (OSPF)

To enable plain text, Message Digest 5 (MD5) authentication, or null authentication for an Open Shortest Path First (OSPF) interface, use the **authentication** command in the appropriate mode. To remove such authentication, use the **no** form of this command.

authentication [{**message-digest** [**keychain** *keychain*] | **null**}]
no authentication

Syntax Description

message-digest	(Optional) Specifies that MD5 is used.
keychain *keychain*	(Optional) Specifies a keychain name.
null	(Optional) Specifies that no authentication is used. Useful for overriding password or MD5 authentication if configured for an area.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the authentication parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the authentication parameter specified for the process.

If this command is not specified at any level, then the interface does not use authentication.

If no keyword is specified, plain text authentication is used.

Command Modes

Interface configuration

Area configuration

Router configuration

Virtual-link configuration

VRF configuration

Multi-area interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **authentication** command to specify an authentication type for the interface, which overrides the authentication specified for the area to which this interface belongs. If this command is not included in the configuration file, the authentication configured in the area to which the interface belongs is assumed (as specified by the area **authentication** command).

The authentication type and password must be the same for all OSPF interfaces that are to communicate with each other through OSPF. If you specified plain text authentication, use the **authentication-key** command to specify the plain text password.

If you enable MD5 authentication with the **message-digest** keyword, you must configure a key with the **message-digest-key** interface command.

To manage the rollover of keys and enhance MD5 authentication for OSPF, you can configure a container of keys called a keychain with each key comprising the following attributes: generate/accept time, key identification, and authentication algorithm. The keychain management feature is always enabled.

Note Changes to the system clock will impact the validity of the keys in the existing configuration.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set authentication for areas 0 and 1 of OSPF routing process 201. Authentication keys are also provided.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# router-id 10.1.1.1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# authentication
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# authentication-key mykey
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf)# area 1
RP/0/RP0:hostname(config-ospf-ar)# authentication
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/6.11
RP/0/RP0:hostname(config-ospf-ar-if)# authentication-key mykey1
```

The following example shows how to configure use of an authentication keychain:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# router-id 10.1.1.1
RP/0/RP0:hostname(config-ospf)# authentication message-digest keychain mykeychain
```

Related Commands

Command	Description
authentication-key (OSPF), on page 229	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
message-digest-key, on page 287	Specifies a key used with OSPF MD5 authentication.

authentication-key (OSPF)

To assign a password to be used by neighboring routers that are using the Open Shortest Path First (OSPF) simple password authentication, use the **authentication-key** command in the appropriate mode. To remove a previously assigned OSPF password, use the **no** form of this command.

authentication-key [{**clear** | **encrypted**}] *password*
no authentication-key

Syntax Description

clear	(Optional) Specifies that the key be clear text.
encrypted	(Optional) Specifies that the key be encrypted using a two-way algorithm.
password	Any contiguous string up to 8 characters in length that can be entered from the keyboard. For example, *mypswd2*.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the OSPF password parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the OSPF password parameter specified for the process.

If this command is not specified at any level, then no password is specified.

Clear is the default if the **clear** or **encrypted** keyword is not specified.

Command Modes

Interface configuration

Area configuration

Router configuration

Virtual-link configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The password created by this command is inserted directly into the OSPF header when the software originates routing protocol packets. A separate password can be assigned to each network on an individual interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

The **authentication-key** command must be used with the **authentication** command. If the **authentication** command is not configured, the password provided by the **authentication-key** command is ignored and no authentication is adopted by the OSPF interface.

Note The **authentication-key** command cannot be used with the **authentication** command when the **message-digest** or **null** keyword is configured.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure an authentication password as the string yourpass:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# authentication-key yourpass
```

Related Commands

Command	Description
authentication (OSPF), on page 227	Specifies authentication type.

auto-cost (OSPF)

To control how the Open Shortest Path First (OSPF) protocol calculates default metrics for the interface, use the **auto-cost** command in the appropriate mode. To revert to the default reference bandwidth, use the **no** form of this command.

auto-cost {**reference-bandwidth** *mbps* | **disable**}
no auto-cost {**reference-bandwidth** | **disable**}

Syntax Description

reference-bandwidth *mbps*	Specifies a rate in Mbps (bandwidth). Range is 1 to 4294967.
disable	Assigns a cost based on interface type.

Command Default

mbps : 100 Mbps

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface.

The OSPF metric is calculated as the *mbps* value divided by bandwidth, with *mbps* equal to 108 by default.

If you have multiple links with high bandwidth (such as OC-192), you might want to use a larger number to differentiate the cost on those links. That is, the metric calculated using the default *mbps* value is the same for all high-bandwidth links.

Recommended usage of cost configuration for OSPF interfaces with high bandwidth is to be consistent: Either explicitly configure (by using the **cost** command) or choose the default (by using the **auto-cost** command).

The value set by the **cost** command overrides the cost resulting from the **auto-cost** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set the reference value for the auto cost calculation to 1000 Mbps:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# auto-cost reference-bandwidth 1000
```

Related Commands

Command	Description
cost (OSPF), on page 242	Explicitly specifies the cost of the interface (network) for OSPF path calculation.

capability opaque disable

To prevent Multiprotocol Label Switching traffic engineering (MPLS TE) topology information flooded to the network through opaque LSAs, use the **capability opaque disable** command in the appropriate mode. To restore MPLS TE topology information flooded through opaque LSAs to the network, use the **no** form of the command.

capability opaque disable
no capability opaque disable

Command Default

Opaque LSAs are allowed.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **capability opaque disable** command prevents flooded MPLS TE information (Types 1 and 4) through opaque LSAs of all scope (Types 9, 10, and 11).

Control opaque LSA support capability must be enabled for OSPF to support MPLS TE.

The MPLS TE topology information is flooded to the area through opaque LSAs by default.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to prevent OSPF from supporting opaque services:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# capability opaque disable
```

clear ospf process

To reset an Open Shortest Path First (OSPF) router process without stopping and restarting it, use the **clear ospf process** command in exec mode.

clear ospf [*process-name* [**vrf** {*vrf-name* | **all**}]] **process**

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF processes are reset.
vrf	(Optional) An OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.

Command Default

No default behavior or value

Command Modes

exec mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the OSPF router process is reset, OSPF releases all resources allocated, cleans up the internal database, and shuts down and restarts all interfaces that belong to the process.

Note The **clear ospf process** command may change the router ID unless the OSPF router ID is explicitly configured through the router-id (OSPF), on page 336 command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to reset all OSPF processes:

```
RP/0/RP0:hostname# clear ospf process
```

The following example shows how to reset the OSPF 1 process:

```
RP/0/RP0:hostname# clear ospf 1 process
```

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.
router-id (OSPF), on page 336	Configures a router ID for the OSPF process.

clear ospf redistribution

To clear all routes redistributed from other protocols out of the Open Shortest Path First (OSPF) routing table, use the **clear ospf redistribution** command in exec mode.

clear ospf [*process-name* [**vrf** {*vrf-name* | **all**}]] **redistribution**

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF routes are cleared.
vrf	(Optional) OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.

Command Default

No default behavior or value

Command Modes

exec

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear ospf redistribution** command to cause the routing table to be read again. OSPF regenerates and sends Type 5 and Type 7 link-state advertisements (LSAs) to its neighbors. If an unexpected route has appeared in the OSPF redistribution, using this command corrects the issue.

Note Use of this command can cause a significant number of LSAs to flood the network. We recommend that you use this command with caution.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to clear all redistributed routes across all processes from other protocols:

```
RP/0/RP0:hostname# clear ospf redistribution
```

clear ospf routes

To clear all Open Shortest Path First (OSPF) routes from the OSPF routing table, use the **clear ospf routes** command in exec mode.

clear ospf [*process-name* [**vrf** {*vrf-name* | **all**}]] **routes**

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF routes are cleared.
vrf	(Optional) OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.

Command Default

No default behavior or value

Command Modes

exec

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to clear all OSPF routes from the OSPF routing table and recompute valid routes. When the OSPF routing table is cleared, OSPF routes in the global routing table are also recalculated.

```
RP/0/RP0:hostname# clear ospf routes
```

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.

clear ospf statistics

To clear the Open Shortest Path First (OSPF) statistics of neighbor state transitions, use the **clear ospf statistics** command in exec mode.

clear ospf [*process-name* [**vrf** {*vrf-name* | **all**}]] **statistics** [**neighbor** [*type interface-path-id*] [*ip-address*]]

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF statistics of neighbor state transitions are cleared.
vrf	(Optional) OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.
neighbor	(Optional) Clears the state transition counters of the specified neighbor only.
type	(Optional) Interface type.
interface-path-id	(Optional) Physical interface or virtual interface. Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
ip-address	(Optional) IP address of a specified neighbor for whom you want to clear the state transition counter.

Command Default

No default behavior or value

Command Modes

exec mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear ospf statistics** command to reset OSPF counters. Reset is useful to detect changes in counter values.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to reset the OSPF transition state counters for all neighbors on Packet-over-SONET/SDH (POS) interface 0/2/0/0:

```
RP/0/RP0:hostname# clear ospf statistics neighbor POS 0/2/0/0
```

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.

clear ospf statistics interface

To clear the Open Shortest Path First (OSPF) statistics per interface, use the **clear ospf statistics interface** command in exec mode.

clear ospf statistics interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or value.

Command Modes

exec mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear ospf statistics interface** command to reset OSPF counters. Reset is useful to detect changes in counter values.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to reset OSPF statistics for interface POS 0/21/0/0:

```
RP/0/RP0:hostname# clear ospf statistics interface POS 0/21/0/0
```

Related Commands

Command	Description
clear ospf statistics, on page 239	Clears the Open Shortest Path First (OSPF) statistics of neighbor state transitions.

cost (OSPF)

To explicitly specify the interface (network) for Open Shortest Path First (OSPF) path calculation, use the **cost** command in the appropriate mode. To remove the cost, use the **no** form of this command.

cost *cost*
no cost

Syntax Description

cost	Unsigned integer value expressed as the link-state metric. Range is 1 to 65535.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the cost parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the cost parameter specified for the process.

If this command is not specified at any level, then the cost is calculated by the **auto-cost** command.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The link-state metric is advertised as the link cost in the router link advertisement. The Cisco IOS XR software does not support type of service (ToS), so you can assign only one cost for each interface.

In general, the path cost is calculated using the following formula:

108 / bandwidth (the default auto cost is set to 100 Mbps)

This calculation is the default reference bandwidth used by the auto-costing calculation which establishes the interface auto-cost The **auto-cost** command can set this reference bandwidth to some other value. The **cost** command is used to override the auto-costing calculated default value for interfaces.

Using this formula, the default path cost is 1 for any interface that has a link bandwidth of 100 Mbps or higher. If this value does not suit the network, configure the reference bandwidth for auto calculating costs based on the link bandwidth.

The value set by the **cost** command overrides the cost resulting from the **auto-cost (OSPF)** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set the cost value to 65 for Ten Gigabit Ethernet interface 0/6/0/2.10:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# cost 65
```

Related Commands

Command	Description
auto-cost (OSPF), on page 231	Controls how the OSPF protocol calculates default metrics for the interface.

cost-fallback (OSPF)

To apply higher cost than the normal interface cost when the cumulative bandwidth of a bundle interface goes below the threshold specified and to revert to the original cost if the cumulative bandwidth goes above the configured threshold, use the **cost-fallback** command. To remove the cost-fallback, use the **no** form of this command.

cost-fallback cost threshold bandwidth
no cost-fallback

Syntax Description

cost **threshold**	Unsigned integer value expressed as the link-state metric. Range is 1 to 65535, but typically, cost-fallback value is supposed to be set to a value higher than the normal cost.
bandwidth	Unsigned integer value expressed in Mbits per second. Range is 1 to 4294967.

Command Default

If this command is not specified in interface configuration mode, the currently effective interface cost takes effect even when the cumulative bandwidth goes down below the maximum bandwidth. Unlike the interface cost command, this cost-fallback command is available only under interface configuration mode; it is not available in area or process level. Unlike other interface specific parameters, no inheritance will take place from area or process level if this command is not specified at interface level.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The fallback cost must be set to a higher value than the normal interface cost. The motivation of setting the fallback cost is to cost out an interface or disfavor an interface without shutting it down when its cumulative bandwidth goes below the user specified threshold, so that the traffic can take an alternative path. The normal interface cost will take over when the cumulative bandwidth reaches or exceeds user-specified threshold.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set the cost-fallback value:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)#router ospf 100
RP/0/RP0:hostname(config-ospf)#router-id 2.2.2.2
```

```
RP/0/RP0:hostname(config-ospf)#area 0
RP/0/RP0:hostname(config-ospf-ar)#interface bundle-a pos1
RP/0/RP0:hostname(config-ospf-ar-if)#cost-fallback 1000 threshold 300
```

Related Commands

Command	Description
auto-cost (OSPF), on page 231	Controls how the OSPF protocol calculates default metrics for the interface.
cost (OSPF), on page 242	Specifies the cost of the interface (network) for OSPF path calculation.

database-filter all out (OSPF)

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) interface, use the **database-filter all out** command in the appropriate mode. To restore the forwarding of LSAs to the interface, use the **disable** form of the command.

database-filter all out [{**disable** | **enable**}]

Syntax Description

disable	(Optional) Disables filtering.
enable	(Optional) Enables filtering.

Command Default

The database filter is disabled.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **database-file all out** command to perform the same function that the neighbor database-filter all out, on page 300 command performs on a neighbor basis.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to prevent flooding of OSPF LSAs to broadcast, nonbroadcast, and point-to-point networks reachable through Ten Gigabit Ethernet interface 0/6/0/2.10:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# database-filter all out
```

dead-interval (OSPF)

To set the interval after which a neighbor is declared dead when no hello packets are observed, use the **dead-interval** command in the appropriate mode. To return to the default time, use the **no** form of this command.

dead-interval *seconds*
no dead-interval

Syntax Description

seconds	Integer that specifies the interval (in seconds). Range is 1 to 65535. The value must be the same for all nodes on the network.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the dead interval parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the dead interval parameter specified for the process.

If this command is not specified at any level, then the dead interval is four times the interval set by the **hello-interval** (OSPF) command.

Command Modes

Interface configuration

Area configuration

Router configuration

Virtual-link configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The dead interval value must be the same for all routers and access servers on a specific network.

If the hello interval is configured, the dead interval value must be larger than the hello interval value. The dead interval value is usually configured four times larger than the hello interval value.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set the OSPF dead interval to 40 seconds:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# dead-interval 40
```

Related Commands

Command	Description
hello-interval (OSPF), on page 271	Specifies the interval between hello packets that the Cisco IOS XR software sends on the interface.

default-cost (OSPF)

To specify a cost for the default summary route sent into a stub area or not-so-stubby area (NSSA), use the **default-cost** command in area configuration mode. To remove the assigned default route cost, use the **no** form of this command.

default-cost *cost*
no default-cost *cost*

Syntax Description

cost	Cost for the default summary route used for a stub or NSSA area. The acceptable value is a 24-bit number.

Command Default

cost : 1

Command Modes

Area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **default-cost** command only on an Area Border Router (ABR) attached to a stub or an NSSA area.

In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **stub** command in the area submode. Use the **default-cost** command only on an ABR attached to the stub area. The **default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to assign a default cost of 20 to a stub area. The Ten Gigabit Ethernet interface 0/6/0/2.10 is also configured in the stub area:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# area 10.15.0.0
RP/0/RP0:hostname(config-ospf-ar)# stub
RP/0/RP0:hostname(config-ospf-ar)# default-cost 20
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Related Commands

Command	Description
stub (OSPF), on page 403	Defines an area as a stub area.

default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the **default-information originate** command in the appropriate mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-policy** *policy-name*] [**tag** *tag-value*]
no default-information originate

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the routing table has a default route.
metric *metric-value*	(Optional) Specifies the metric used for generating the default route. The default metric value is 1. Range is 1 to 16777214.
metric-type *type-value*	(Optional) Specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: **1**—Type 1 external route **2**—Type 2 external route
tag *tag-value*	(Optional) 32-bit dotted-decimal value attached to each external route. This is not used by the OSPF protocol itself. It may be used to communicate information between autonomous system boundary routers (ASBRs). If a tag is not specified, then the configured OSPF process number is used.
route-policy *policy-name*	(Optional) Specifies that a routing policy be used and the routing policy name.

Command Default

When you do not use this command in router configuration mode, no default external route is generated into an OSPF routing domain.

metric-value : 1

type-value : 2

tag-value: configured OSPF process number

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Whenever you use the **redistribute** or **default-information originate** command to redistribute routes into an OSPF routing domain, the software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

The **default-information originate** route-policy attach point conditionally injects the default route 0.0.0.0/0 into the OSPF link-state database, and is done by evaluating the attached policy. If any routes specified in the policy exist in the global RIB, then the default route is inserted into the link-state database. If there is no match condition specified in the policy, the policy passes and the default route is generated into the link-state database.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 109
RP/0/RP0:hostname(config-ospf)#redistribute igrp 108 metric 100
RP/0/RP0:hostname(config-ospf)#default-information originate metric 100 metric-type 1
```

Related Commands

Command	Description
redistribute (OSPF), on page 329	Redistributes routes from one routing domain into a specified OSPF process.

default-metric (OSPF)

To set default metric values for routes redistributed from another protocol into the Open Shortest Path First (OSPF) protocol, use the **default-metric** command in the appropriate mode. To return to the default state, use the **no** form of this command.

default-metric *value*
no default-metric *value*

Syntax Description

value	Default metric value appropriate for the specified routing protocol. Range is 1 to 16777214.

Command Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **default-metric** command with the **redistribute** command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, use a default metric to provide a reasonable substitute and enable the redistribution to proceed.

The default-metric value configured in OSPF configuration does not apply to connected routes that are redistributed to OSPF using the **redistribute connected** command. To set a non-default metric for connected routes, configure OSPF with the **redistribute connected metric** *metric-value* command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to advertise Intermediate System-to-Intermediate System (IS-IS) protocol-derived routes into OSPF and assign a metric of 10:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# default-metric 10
RP/0/RP0:hostname(config-ospf)# redistribute isis IS-IS_isp
```

Related Commands

Command	Description
redistribute (OSPF), on page 329	Redistributes routes from one routing domain into a specified OSPF process.

disable-dn-bit-check

To specify that down bits should be ignored, use the **disable-dn-bit-check** command in VPN routing and forwarding (VRF) configuration mode. To specify that down bits should be considered, use the **no** form of this command.

disable-dn-bit-check
no disable-dn-bit-check

Command Default

Down bits are considered.

Command Modes

VRF configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify that down bits be ignored:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# vrf v1
RP/0/RP0:hostname(config-ospf-vrf)# disable-dn-bit-check
```

distance (OSPF)

To define an administrative distance, use the **distance** command in an appropriate configuration mode. To remove the **distance** command from the configuration file and restore the system to its default condition in which the software removes a distance definition, use the **no** form of this command.

distance *weight* [*ip-address wildcard-mask* [*access-list-name*]]
no distance *weight ip-address wildcard-mask* [*access-list-name*]

Syntax Description

weight	Administrative distance. Range is 10 to 255. Used alone, the *weight* argument specifies a default administrative distance that the software uses when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table.
ip-address	(Optional) IP address in four-part, dotted-decimal notation.
wildcard-mask	(Optional) Wildcard mask in four-part, dotted decimal format. A bit set to 1 in the *mask* argument instructs the software to ignore the corresponding bit in the address value.
access-list-name	(Optional) Name of an IP access list to be applied to incoming routing updates.

Command Default

If this command is not specified, then the administrative distance is the default.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An administrative distance is an integer from 10 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

If an access list is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows you to filter networks based on the IP prefix supplying the routing information. For example, you could filter possibly incorrect routing information from networking devices not under your administrative control.

The order in which you enter **distance** commands can affect the assigned administrative distances in unexpected ways (see the “Examples” section for further clarification).

This table lists default administrative distances.

Table 1: Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route out on interface	0
State route to next-hop	1
EIGRP Summary Route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP version 1 and 2	120
External EIGRP	170
Internal BGP	200
Unknown	255

Task ID

Task ID	Operations
ospf	read, write

Examples

In the following example, the **router ospf** command sets up OSPF routing instance1. The first **distance** command sets the default administrative distance to 255, which instructs the software to ignore all routing updates from networking devices for which an explicit distance has not been set. The second **distance** command sets the administrative distance for all networking devices on the Class C network 192.168.40.0 0.0.0.255 to 90.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# distance 255
RP/0/RP0:hostname(config-ospf)# distance 90 192.168.40.0 0.0.0.255
```

Related Commands

Command	Description
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a BGP node.
distance ospf	Allows the use of external, internal, and local administrative distances that could be a better route to an OSPF node.
router ospf, on page 338	Configures the OSPF routing process.

distance ospf

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the **distance ospf** command in router configuration mode. To restore the default value, use the **no** form of this command.

distance ospf {**intra-area** | **inter-area** | **external**} *distance*
no distance ospf

Syntax Description

intra-area | **inter-area** | **external**	Sets the type of area. It can be one of the following values: **intra-area** —All routes within an area. **inter-area** —All routes from one area to another area. **external** —All routes from other routing domains, learned by redistribution. Any combination of the above areas is allowed.
distance	Route administrative distance.

Command Default

distance : 110

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You must specify one of the keywords.

Use the **distance ospf** command to perform the same function as the **distance** command used with an access list. However, the **distance ospf** command sets a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the **distance ospf** command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to change the external distance to 200, making the route less reliable:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# redistribute ospf 2
RP/0/RP0:hostname(config-ospf)# distance ospf external 200
RP/0/RP0:hostname(config-ospf)# exit
RP/0/RP0:hostname(config)# router ospf 2
RP/0/RP0:hostname(config-ospf)# redistribute ospf 1
RP/0/RP0:hostname(config-ospf)# distance ospf external 200
```

Related Commands

Command	Description
disable-dn-bit-check, on page 255	Defines an administrative distance.

distribute-list

To filter networks received or transmitted in Open Shortest Path First (OSPF) updates, use the **distribute-list** command in the appropriate mode. To change or cancel the filter, use the **no** form of this command.

distribute-list {*access-list-name* {**in** | **out** [{**bgp** *number* | **connected** | **ospf** *instance* | **static**}]} | **route-policy** *route-policy-name* **in**}
no distribute-list {*access-list-name* {**in** | **out**} | **route-policy** *route-policy-name* **in**}

Syntax Description

access-list-name	Standard IP access list name. The list defines which networks are to be received and which are to be suppressed in routing updates.
in	Applies the access list or route-policy to incoming routing updates.
out	Applies the access list to outgoing routing updates. The **out** keyword is available only in router configuration mode.
bgp	(Optional) Applies the access list to BGP routes.
connected	(Optional) Applies the access list to connected routes.
ospf	(Optional) Applies the access list to OSPF routes (not the current OSPF process).
static	(Optional) Applies the access list to statically configured routes.
route-policy *route-policy-name*	Specifies the route-policy to filter OSPF prefixes.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the distribute list parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the distribute list parameter specified for the process.

If this command is not specified at any level, then the distribute list is disabled.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **distribute-list** command to limit which OSPF routes are installed on this router. The **distribute-list** command does not affect the OSPF protocol itself.

The **distribute-list in** is configurable at instance (process), area, and interface levels. Regular OSPF configuration inheritance applies. Configuration is inherited from instance > area > interface levels.

Use the **route-policy** *route-policy-name* keyword and argument to allow use of route policies to filter OSPF prefixes.

Note Either an access-list, or a route-policy can be used in a single command, not both. Configuring the command with access-list removes the route-policy configuration, and vice versa.

The "if tag..." statements can be used in **distribute-list in** *route-policy*. The matching on route route tag supports operators "eq/ge/is/le". Operator "in" is not supported.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to prevent OSPF routes from the 172.17.10.0 network from being installed if they are learned in area 0:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ipv4 access-list 3
RP/0/RP0:hostname(config-ipv4-acl)# deny 172.17.10.0 0.0.0.255
RP/0/RP0:hostname(config-ipv4-acl)# permit any any
!
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# distribute-list 3 in
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

domain-id (OSPF)

To specify the Open Shortest Path First (OSPF) VPN routing and forwarding (VRF) domain ID, use the **domain-id** command in VRF configuration mode. To remove an OSPF VRF domain ID, use the **no** form of this command.

domain-id [**secondary**] **type** [{**0005** | **0105** | **0205** | **8005**}] **value** *value*
no domain-id [**secondary**] **type** [{**0005** | **0105** | **0205** | **8005**}] **value** *value*

Syntax Description

secondary	(Optional) OSPF secondary domain ID.
type	Primary OSPF domain ID in hex format.
value *value*	OSPF domain ID value in hex format (six octets).

Command Default

No domain ID is specified.

Command Modes

VRF configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An OSPF domain id must be explicitly configured. The OSPF domain ID helps OSPF determine how to translate a prefix received through Border Gateway Protocol (BGP) from the remote provider edge (PE). If the domain IDs match, OSPF generates a Type 3 link state advertisement (LSA). If the domain IDs do not match, OSPF generates a Type 5 LSA.

There is only one primary domain ID. There can be multiple secondary domain IDs.

Note When an IOS XR router and an IOS router are configured as peers, the two Domain IDs must match. Manually configure the IOS XR Domain ID value to match the IOS default Domain ID value. This ensures that the routes have route code "OIA" because they are learned as inter-area routes. If the Domain IDs do not match, the routes have route code, "O-E2" because they are learned as external routes. Use the **show ip ospf** command to get the OSPF Domain ID from the IOS router. Then, set the IOS XR Domain ID to the same value using the **domain-id** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify a domain ID:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf o1
RP/0/RP0:hostname(config-ospf)# vrf v1
RP/0/RP0:hostname(config-ospf-vrf)# domain-id type 0105 value AABBCCDDEEFF
```

fast-reroute (OSPFv2)

To enable IP fast reroute loop-free alternate (LFA) computation, use the **fast-reroute** command in the appropriate OSPF configuration mode. To disable the IP fast reroute loop-free alternate computation, use the **no** form of this command.

To disable loop-free alternate computation that is enabled on a higher level, use the **fast-reroute** command with **disable** keyword.

fast-reroute {**per-link** | **per-prefix**} [**disable**]
no fast-reroute

Syntax Description

per-link	Enables per-link loop-free alternate computation.
per-prefix	Enables per-prefix loop-free alternate computation.
disable	(Optional) Disables loop-free alternate computation that was enabled on a higher level.

Command Default

IP fast-reroute LFA computation is disabled.

Command Modes

Area configuration

Interface configuration

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Only one mode of computation can be configured on an interface - per-link or per-prefix. Different modes of computations can be enabled on different interfaces; one set of interface using per-link and other set using per-prefix computation. Based on the outgoing interface of the primary path, per-link or per-prefix backup path will be computed.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to enable per-link computation of loop-free alternates under interface 0/6/0/2.10:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# fast-reroute per-link
```

This example shows how to enable per-prefix computation of loop-free alternates under area 0:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 1
RP/0/RP0:hostname(config-ospf)#area 0
RP/0/RP0:hostname(config-ospf-ar)#fast-reroute per-prefix
```

This example shows how to disable computation of loop-free alternates that was configured under area 0:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 1
RP/0/RP0:hostname(config-ospf)#area 0
RP/0/RP0:hostname(config-ospf-ar)#fast-reroute per-prefix
RP/0/RP0:hostname(config-ospf-ar)#interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)#fast-reroute disable
```

fast-reroute per-link exclude interface

To excludes specified interface to be used as a backup during (IPFRR) loop-free alternate (LFA) computation, use the **fast-reroute per-link exclude interface** command, in the appropriate OSPF configuration mode. To disable this feature, use the **no** form of this command.

fast-reroute per-link exclude interface *type interface-path-id*
no fast-reroute per-link exclude interface *type interface-path-id*

Syntax Description

type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

No interfaces are excluded.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to exclude an interface from IP fast reroute loop-free alternate (LFA) computation:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf-ar-if)# fast-reroute per-link exclude interface
TenGigE0/6/0/2.10
```

Related Commands

Command	Description
fast-reroute (OSPFv2), on page 265	Enables IP fast reroute loop-free alternate (LFA) computation.

fast-reroute per-prefix exclude interface (OSPFv2)

To exclude interface to be used as a backup path from fast-reroute loop-free alternate per-prefix computation, use the **fast-reroute per-prefix exclude interface** command in the appropriate OSPF configuration mode. To disable this feature, use the **no** form of this command.

fast-reroute per-prefix exclude interface *type interface-path-id*
no fast-reroute per-prefix exclude interface *type interface-path-id*

Syntax Description

type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router.

Command Default

No interfaces are excluded.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Backup paths via the excluded interfaces will not be computed.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to exclude interface POS0/6/0/1 from being used as a backup path:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 100
RP/0/RP0:hostname(config-ospf)#fast-reroute per-prefix exclude interface TenGigE0/6/0/2.10
```

fast-reroute per-prefix lfa-candidate (OSPFv2)

To add interfaces to the LFA candidate list, use the **fast-reroute per-prefix lfa-candidate** command in interface configuration mode. To disable this feature, use the **no** form of this command.

fast-reroute per-prefix lfa-candidate [*interface-name*]
no fast-reroute per-prefix lfa-candidate [*interface-name*]

Syntax Description

interface-name	Specifies name of the interface to add to the LFA candidate list.

Command Default

No interfaces are added to the candidate list.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to add an interface to LFA candidates:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 100
RP/0/RP0:hostname(config-ospf)#fast-reroute per-prefix lfa-candidate interface
TenGigE0/1/1/0.31
```

hello-interval (OSPF)

To specify the interval between consecutive hello packets that are sent on the Open Shortest Path First (OSPF) interface, use the **hello-interval** command in the appropriate mode. To return to the default time, use the **no** form of this command.

hello-interval *seconds*
no hello-interval

Syntax Description

seconds	Interval (in seconds). The value must be the same for all nodes on a specific network. Range is 1 to 65535.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the hello interval parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the hello interval parameter specified for the process.

If this command is not specified at any level, then the hello interval is 10 seconds (broadcast) or 30 seconds (non-broadcast).

Command Modes

Interface configuration

Area configuration

Router configuration

Virtual-link configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The hello interval value is advertised in the hello packets. The shorter the hello interval, the faster topological changes are detected, but more routing traffic occurs. This value must be the same for all routers and access servers on a specific network.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set the interval between hello packets to 15 seconds:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# hello-interval 15
```

Related Commands

Command	Description
dead-interval (OSPF), on page 247	Sets the time period for which hello packets are suspended before neighbors declare the router down.

interface (OSPF)

To define the interfaces on which the Open Shortest Path First (OSPF) protocol runs, use the **interface** command in area configuration mode. To disable OSPF routing for interfaces, use the **interface** form of this command.

interface *type interface-path-id*
no interface *type interface-path-id*

Syntax Description

type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** se the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

When you do not specify this command in configuration mode, OSPF routing for interfaces is not enabled.

Command Modes

Area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **interface** command to associate a specific interface with an area. The interface remains associated with the area even when the IP address of the interface changes.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how the OSPF routing process 109 defines four OSPF areas (0, 2, 3, and 10.9.50.0), and associates an interface with each area:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/14/0/3.50
!
RP/0/RP0:hostname(config-ospf)# area 2
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE1/0/0/3.50
!
```

```
RP/0/RP0:hostname(config-ospf)# area 3
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
!
RP/0/RP0:hostname(config-ospf)# area 10.9.50.0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/6.11
```

log adjacency changes (OSPF)

To configure the router to send a syslog message when the state of an Open Shortest Path First (OSPF) neighbor changes, use the **log adjacency changes** command in router configuration mode. To turn off this function, use the **disable** keyword. To log all state changes, use the **detail** keyword.

log adjacency changes {**detail** | **disable**}

Syntax Description

detail	Provides all (DOWN, INIT, 2WAY, EXSTART, EXCHANGE, LOADING, FULL) adjacency state changes.
disable	Disables sending adjacency change messages.

Command Default

The router sends a syslog message when the state of an OSPF neighbor changes.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **log adjacency changes** command to display high-level changes to the state of the peer relationship. Configure this command if you want to know about OSPF neighbor changes.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the software to send a syslog message for any OSPF neighbor state changes:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# log adjacency changes detail
```

loopback stub-network

To enable advertising loopback as stub networks, use the **loopback stub-network** command in an appropriate configuration mode. To disable advertising loopback as stubnetworks, use the **no** form of this command.

loopback stub-network [{**enable** | **disable**}]
no loopback stub-network

Syntax Description

enable	(Optional) Enables advertising loopbacks as stub networks.
disable	(Optional) Disables advertising loopbacks as stub networks.

Command Default

By default, OSPF advertises loopbacks as stub hosts.

Command Modes

OSPF interface configuration

OSPF router configuration

OSPF area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In the interface submode, the command can be enabled only on loopback interfaces.

Task ID

Task ID	Operation
ospf	read, write

Examples

The following example shows how to enable advertising loopback as a stub network, under OSPF interface configuration:

```
RP/0/RP0:hostname(config)#router ospf 100
RP/0/RP0:hostname(config-ospf)#loopback stub-network enable
```

Related Commands

Command	Description
show ospf interface, on page 361	Displays Open Shortest Path First (OSPF) interface information.

max-lsa

To limit the number of nonself-generated link-state advertisements (LSAs) that an Open Shortest Path First (OSPF) routing process can keep in the OSPF link-state database (LSDB), use the **max-lsa** command in router configuration mode. To remove the limit of non self-generated LSAs that an OSPF routing process can keep in the OSPF LSDB, use the **no** form of this command.

max-lsa *max* [*threshold*] [**warning-only**] [**ignore-time** *value*] [**ignore-count** *value*] [**reset-time** *value*]
no max-lsa *max* [*threshold*] [**warning-only**] [**ignore-time** *value*] [**ignore-count** *value*] [**reset-time** *value*]

Syntax Description

max	Maximum number of nonself-generated LSAs the OSPF process can keep in the OSPF LSBD.
threshold	(Optional) The percentage of the maximum LSA number, as specified by the maximum-number argument, at which a warning message is logged. The default is 75 percent.
warning-only	(Optional) Specifies that only a warning message is sent when the maximum limit for LSAs is exceeded. Disabled by default.
ignore-time *value*	(Optional) Specifies the time, in minutes, to ignore all neighbors after the maximum limit of LSAs has been exceeded. The default is 5 minutes.
ignore-count *value*	(Optional) Specifies the number of times the OSPF process can consecutively be placed into the ignore state. The default is 5 times.
reset-time *value*	(Optional) Specifies the time, in minutes, after which the ignore count is reset to zero. The default is 2 times **ignore-time** .

Command Default

Disabled

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command allows you to protect the OSPF routing process from the large number of received LSAs that can result from a misconfiguration on another router in the OSPF domain (for example, the redistribution of a large number of IP prefixes to OSPF).

When this feature is enabled, the router keeps count of the number of all received (nonself-generated) LSAs. When the configured *threshold* value is reached, an error message is logged. When the configured *max* number of received LSAs is exceeded, the router stops accepting new LSAs.

If the count of received LSAs is higher than the configured *max* number after one minute, the OSPF process disables all adjacencies in the given context and clears the OSPF database. This state is called the ignore state. In this state, all OSPF packets received on all interfaces belonging to the OSPF instance are ignored and no OSPF packets are generated on its interfaces. The OSPF process remains in the ignore state for the duration of the configured **ignore-time** . When the **ignore-time** expires, the OSPF process returns to normal operation and starts building adjacencies on all its interfaces.

To prevent the OSPF instance from endlessly oscillating between its normal state and the ignore state, as a result of the LSA count immediately exceeding the *max* number again after it returns from the ignore state, the OSPF instance keeps a count of how many times it has been in the ignore state. This counter is called the **ignore-count** . If the **ignore-count** exceeds its configured value, the OSPF instance remains in the ignore state permanently.

To return the OSPF instance to its normal state, you must issue the **clear ip ospf** command. The **ignore-count** is reset to zero if the LSA count does not exceed the *max* number again during the time configured by the **reset-time** keyword.

If you use the **warning-only** keyword, the OSPF instance never enters the ignore state. When LSA count exceeds the *max* number, the OSPF process logs an error message and the OSPF instance continues in its normal state operation.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the OSPF instance to accept 12000 nonself-generated LSAs in the global routing table, and 1000 nonself-generated LSAs in VRF V1.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 0
RP/0/RP0:hostname(config-ospf)# max-lsa 12000
RP/0/RP0:hostname(config-ospf)# vrf V1
RP/0/RP0:hostname(config-ospf)# max-lsa 1000
```

The following example shows how to display the current status of the OSPF instance:

```
RP/0/RP0:hostname# show ospf 0

  Routing Process "ospf 0" with ID 10.0.0.2
  NSR (Non-stop routing) is Disabled
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  It is an area border router
  Maximum number of non self-generated LSA allowed 12000
     Current number of non self-generated LSA 1
     Threshold for warning message 75%
     Ignore-time 5 minutes, reset-time 10 minutes
     Ignore-count allowed 5, current ignore-count 0
```

Related Commands

Command	Description
show ospf, on page 340	Displays general information about Open Shortest Path First (OSPF) routing processes.

max-metric

To configure the Open Shortest Path First (OSPF) protocol to signal other networking devices not to prefer the local router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric** command in router configuration mode. To disable this function, use the **no** form of this command.

max-metric router-lsa [**external-lsa** *overriding metric*] [**include-stub**] [**on-proc-migration**] [**on-proc-restart**] [**on-startup**] [**on-switchover**] [**wait-for-bgp**] [**summary-lsa**]
no max-metric router-lsa

Syntax Description

router-lsa	Always originates router link-state advertisements (LSAs) with the maximum metric.
external-lsa *overriding metric*	(Optional) Overrides the external-lsa metric with the max-metric value.The *overriding metric* argument specifies the number of in-summary-LSAs. The range is 1 to 16777215>. The default is 16711680.
include-stub	(Optional) Advertises stub links in router-LSA with the max-metric value (0xFFFF).
on-proc-migration *time*	(Optional) Sets the maximum metric temporarily after a process migration to originate router-LSAs with the max-metric value. The *time* range is 5 to 86400 seconds.
on-proc-restart *time*	(Optional) Sets the maximum metric temporarily after a process restart to originate router-LSAs with the max-metric value. The *time* range is 5 to 86400 seconds.
on-startup *time*	(Optional) Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value. The *time* range is 5 to 86400 seconds.
on-switchover *time*	(Optional) Sets the maximum metric temporarily after a switchover to originate router-LSAs with the max-metric value. The *time* range is 5 to 86400 seconds. **Note** OSPF will not populate maximum metric on the router's generated LSAs, when the OSPF routing process is configured to support Nonstop Routing (NSR) or Nonstop Forwarding/Graceful restart (NSF/GR).
wait-for-bgp	(Optional) Causes OSPF to originate router LSAs with the maximum metric and allows Border Gateway Protocol (BGP) to decide when to start originating router LSAs with a normal metric instead of the maximum metric.
summary-lsa	(Optional) specifies the number of in summary-LSAs. The range is 1 to 16777215. The default is 16711680.

Command Default

Router LSAs are originated with normal link metrics.

overriding-metric :16711680

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **max-metric** command to cause the software to originate router LSAs with router link metrics set to LSInfinity (0XFFFF). This feature can be useful in Internet backbone routers that run both OSPF and BGP because OSPF converges more quickly than BGP and may begin attracting traffic before BGP has converged, resulting in dropped traffic.

If this command is configured, the router advertises its locally generated router LSAs with a metric of 0XFFFF. This action allows the router to converge but not attract transit traffic if there are better, alternative paths around this router. After the specified *announce-time* value or notification from BGP has expired, the router advertises the local router LSAs with the normal metric (interface cost).

If this command is configured with the **on-startup** keyword, then the maximum metric is temporarily set only after reboot is initiated. If this command is configured without the **on-startup** keyword, then the maximum metric is permanently used until the configuration is removed.

If the **include-stub** keyword is enabled, the stub-links in the router LSA will be sent with the max-metric. If the **summary-lsa** keyword is enabled, all self-generated summary LSAs will have a metric set to 0xFF0000, unless the metric value is specified with the max-metric value parameter. If the **external-lsa** keyword is enabled, all self-generated external LSAs will have a metric set to 0xFF0000, unless the metric value is specified with the max-metric value parameter.

This command might be useful when you want to connect a router to an OSPF network, but do not want real traffic flowing through it if there are better, alternative paths. If there are no alternative paths, this router still accepts transit traffic as before.

Some cases where this command might be useful are as follows:

- During a router reload, you prefer that OSPF wait for BGP to converge before accepting transit traffic. If there are no alternative paths, the router still accepts transit traffic.
- A router is in critical condition (for example, it has a very high CPU load or does not have enough memory to store all LSAs or build the routing table).
- When you want to gracefully introduce or remove a router to or from the network.
- When you have a test router in a lab, connected to a production network.

Note For older OSPF implementations (RFC 1247), router links in received router LSAs with a metric and cost of LSInfinity are not used during SPF calculations. Hence, no transit traffic is set to the routers originating such router LSAs.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure OSPF to originate router LSAs with the maximum metric until BGP indicates that it has converged:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# max-metric router-lsa on-startup wait-for-bgp
```

maximum interfaces (OSPF)

To limit the number of interfaces that can be configured for an Open Shortest Path First (OSPF) process, use the **maximum interfaces** command in the appropriate mode. To return to the default limit, use the **no** form of this command.

maximum interfaces *number-interfaces*
no maximum interfaces

Syntax Description

number-interfaces	Number of interfaces. Range is 1 to 1024.Range is 1 to 4294967295.

Command Default

If the command is not specified, the default is 255.

If the command is not specified, the default is 1024.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **maximum interface** command to increase or decrease the limit on the number of interfaces configured for an OSPF process.

You cannot configure a limit lower than the number of interfaces currently configured for the OSPF process. To lower the limit, remove interfaces from the OSPF configuration until the number of configured interfaces is at or below the desired limit. You may then apply the new, lower limit.

Task ID

Task ID	Operations
ospf	read, write

Examples

This example shows how to configure a maximum interface limit of 700 on a router:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# maximum interfaces 700
```

This example shows how to configure a maximum interface limit of 1500 on a router:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# maximum interfaces 1500
```

Related Commands

Command	Description
show ospf interface, on page 361	Displays OSPF interface information.

maximum redistributed-prefixes (OSPF)

To limit the aggregate number of prefixes that can be redistributed into an Open Shortest Path First (OSPF) process, use the **maximum redistributed-prefix** command in the appropriate mode. To return to the default limit, use the **no** form of this command.

maximum redistributed-prefixes *maximum* [*threshold-value*] [**warning-only**]
no maximum redistributed-prefixes

Syntax Description

maximum	Number of routes. Range is 1 to 4294967295.
threshold-value	(Optional) Threshold value (as a percentage) at which to generate a warning message. Range is 1 to 100.
warning-only	(Optional) Gives only a warning when the limit is exceeded.

Command Default

If the command is not specified, the default is 10000.

The threshold value defaults to 75 percent.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **maximum redistributed-prefixes** command to increase or decrease the maximum number of prefixes (also referred to as routes) redistributed for an OSPF process.

If the *maximum* value is less than the existing number of routes, existing routes remain configured, but no new routes are redistributed.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure a maximum number of routes that can be redistributed for an OSPF routing process:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
```

```
RP/0/RP0:hostname(config-ospf)# maximum redistributed-prefixes 15000
```

Related Commands

Command	Description
show ospf routes, on page 384	Displays the OSPF topology table.

message-digest-key

To specify a key used with Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the **message-digest-key** command in the appropriate mode. To remove an old MD5 key, use the **no** form of this command.

message-digest-key *key-id* **md5** {*key* | **clear** *key* | **encrypted** *key*}
no message-digest-key *key-id*

Syntax Description

key-id	Key number. Range is 1 to 255.
md5	Enables OSPF MD5 authentication.
key	Alphanumeric string of up to 16 characters.
clear	Specifies that the key be clear text.
encrypted	Specifies that the key be encrypted using a two-way algorithm.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the message digest key parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the message digest key parameter specified for the process.

If this command is not specified at any level, then OSPF MD5 authentication is disabled.

Command Modes

Interface configuration

Area configuration

Router configuration

Virtual-link configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Usually, one key individual interface is used to generate authentication information when packets are sent and to authenticate incoming packets. The same key identifier on the neighbor router must have the same *key* value.

For authentication to be enabled, you must configure the **message-digest-key** command together with the **authentication** command and its **message-digest** keyword. Both the **message-digest-key** and **authentication** commands can be inherited from a higher configuration level.

The process of changing keys is as follows. Suppose the current configuration is:

```
interface TenGigE0/6/0/2.10
 message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface TenGigE0/6/0/2.10
 message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops after the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
 no ospf message-digest-key 100
```

Then, only key 101 is used for authentication on interface 1.

We recommend that you not keep more than one key individual interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

Note The MD5 key is always stored in encrypted format on the router. The **clear** and **encrypted** keywords inform the router whether the value that is entered is encrypted or unencrypted.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set a new key 19 with the password *8ry4222* :

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# area 0

RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-if)# message-digest-key 19 md5 8ry4222
```

Related Commands

Command	Description
area (OSPF), on page 225	Configures an OSPF area.
authentication (OSPF), on page 227	Enables plain text, MD5 authentication, or null authentication for an OSPF interface.
default-cost (OSPF), on page 249	Enables authentication for an OSPF area.

mpls traffic-eng (OSPF)

To configure an Open Shortest Path First (OSPF) area for Multiprotocol Label Switching traffic engineering (MPLS TE), use the **mpls traffic-eng** command in the appropriate configuration mode. To remove the MPLS TE from an area, use the **no** form of this command.

mpls traffic-eng
no mpls traffic-eng

Syntax Description

This command has no keywords or arguments.

Command Default

MPLS TE is not configured for OSPF.

Command Modes

Area configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You must configure the **mpls traffic-eng** command for OSPF to support MPLS traffic engineering. OSPF provides the flooding mechanism that is used to flood TE link information.

Note This command is supported only in the default VRF mode.

We recommend that you configure the **mpls traffic-eng router-id** command instead of using the **router-id** command in config mode.

OSPF support for MPLS TE is a component of the overall MPLS TE feature. Other MPLS TE software components must also be configured for this feature to be fully supported.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to associate loopback interface 0 with area 0, and area 0 is declared to be an MPLS area:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
```

```
RP/0/RP0:hostname(config-ospf)# router-id 10.10.10.10
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng router-id loopback 0
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng
RP/0/RP0:hostname(config-ospf-ar)# interface loopback 0
```

Related Commands

Command	Description
capability opaque disable, on page 233	Controls the OSPF opaque LSA support capability.
router-id (OSPF), on page 336	Configures a router ID for the OSPF process.

mpls traffic-eng router-id (OSPF)

To specify that the traffic engineering router identifier for the node is the IP address associated with a given Open Shortest Path First (OSPF) interface, use the **mpls traffic-eng router-id** command in the appropriate configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng router-id {*router-id* | *type interface-path-id*}
no mpls traffic-eng router-id {*router-id* | *type interface-path-id*}

Syntax Description

router-id	The 32-bit router ID value specified in four-part, dotted-decimal notation (must be in the valid IP address range of 0.0.0.0 to 255.255.255.255).
type	Interface type.
interface-path-id	Physical interface or virtual interface. Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

If this command is specified in router configuration mode, then the traffic engineering router identifier for the node is the IP address associated with a given interface.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This identifier of the router acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all 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.

Note We recommend that loopback interfaces be used for Multiprotocol Label Switching traffic engineering (MPLS TE), because they are more stable than physical interfaces.

Note This command is supported only in the default VRF mode.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with loopback interface 0:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng router-id loopback 0
```

Related Commands

Command	Description
mpls traffic-eng (OSPF), on page 290	Configures an OSPF area for MPLS TE.

mtu-ignore (OSPF)

To prevent Open Shortest Path First (OSPF) from checking whether neighbors are using the same maximum transmission unit (MTU) on a common interface when exchanging database descriptor (DBD) packets, use the **mtu-ignore** command in the appropriate mode. To reset to default, use the **no** form of this command.

mtu-ignore [{**disable** | **enable**}]
no mtu-ignore

Syntax Description

disable	(Optional) Enables checking for whether OSPF neighbors are using the MTU on a common interface.
enable	(Optional) Disables checking for whether OSPF neighbors are using the MTU on a common interface.

Command Default

The default is **mtu-ignore** with no keywords, which disables MTU checking.

If this command is not specified in interface configuration mode,

then the interface adopts the MTU ignore parameter specified by the area.

If this command is not specified in area configuration mode,

then the interface adopts the MTU ignore parameter specified for the process.

If this command is not specified at any level,

then OSPF checks the MTU received from neighbors when exchanging DBD packets.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

OSPF checks whether OSPF neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the MTU configured on the incoming interface, OSPF adjacency is not established.

The keywords, **disable** and **enable** , do not need to be used. If no keywords are used, the **mtu-ignore** command disables MTU checking. You can then use the **no mtu-ignore** command to activate MTU checking.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to disable MTU mismatch detection on receiving DBD packets:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-if)# mtu-ignore
```

multi-area-interface

To enable multiple adjacencies for different Open Shortest Path First (OSPF) areas and enter multi-area interface configuration mode, use the **multi-area-interface** command in the area configuration mode. To reset to the default, use the **no** form of this command.

multi-area-interface *type interface-path-id*
no multi-area-interface *type interface-path-id*

Syntax Description

type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

An OSPF network is enabled for one area only.

Command Modes

Area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **multi-area-interface** command to enable area border routers (ABRs) to establish multiple adjacencies for different OSPF areas.

Each multiple area adjacency is announced as a point-to-point unnumbered link in the configured area. This point-to-point link provides a topological path for that area. The first or primary adjacency using the link advertises the link consistent with draft-ietf-ospf-multi-area-adj-06.txt.

You can configure multi-area adjacency on any interface where only two OSF speakers are attached. In the case of native broadcast networks, the interface must be configured as an OPSF point-to-point type using the **network point-to-point** command to enable the interface for a multi-area adjacency.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to enable multiple area adjacency for OSPF 109:

```
RP/0/RP0:hostname# configure
```

```
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-if)# area 1
RP/0/RP0:hostname(config-ospf-ar)# multi-area-interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-mif)# ?

    authentication       Enable authentication
    authentication-key   Authentication password (key)
    commit               Commit the configuration changes to running
    cost                 Interface cost
    database-filter      Filter OSPF LSA during synchronization and flooding
    dead-interval        Interval after which a neighbor is declared dead
    describe             Describe a command without taking real actions
    distribute-list      Filter networks in routing updates
    do                   Run an exec command
    exit                 Exit from this submode
    hello-interval       Time between HELLO packets
    message-digest-key   Message digest authentication password (key)
    mtu-ignore           Enable/Disable ignoring of MTU in DBD packets
    no                   Negate a command or set its defaults
    packet-size          Customize size of OSPF packets upto MTU
    pwd                  Commands used to reach current submode
    retransmit-interval  Time between retransmitting lost link state advertisements
    root                 Exit to the global configuration mode
    show                 Show contents of configuration
    transmit-delay       Estimated time needed to send link-state update packet
RP/0/RP0:hostname(config-ospf-ar-mif)#
```

Related Commands

Command	Description
show ospf interface, on page 361	Displays OSPF interface information.

neighbor (OSPF)

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

neighbor *ip-address* [**cost** *number*] [**priority** *number*] [**poll-interval** *seconds*]
no neighbor *ip-address* [**cost** *number*] [**priority** *number*] [**poll-interval** *seconds*]

Syntax Description

ip-address	Interface IP address of the neighbor.
cost *number*	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured assume the cost of the interface, based on the **cost** command. On point-to-multipoint interfaces, **cost** *number* is the only keyword and argument combination that works. The **cost** keyword does not apply to nonbroadcast multiaccess (NBMA) networks.
priority *number*	(Optional) Specifies an 8-bit number indicating the router priority value of the nonbroadcast neighbor associated with the IP address specified. The **priority** keyword does not apply to point-to-multipoint interfaces.
poll-interval *seconds*	(Optional) Specifies an unsigned integer value (in seconds) reflecting the poll interval. RFC 1247 recommends that this value be much larger than the hello interval. The **poll-interval** keyword does not apply to point-to-multipoint interfaces.

Command Default

No configuration is specified.

priority *number* : 0

poll-interval *seconds* : 120 seconds (2 minutes)

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You must include one neighbor entry in the software configuration for each known nonbroadcast network neighbor. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive (hello packets have not been received for the router dead interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets are sent at a reduced rate called the *poll interval*.

When the router starts up, it sends only hello packets to those routers with nonzero priority; that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, the DR and BDR start sending hello packets to all neighbors to form adjacencies.

To filter all outgoing OSPF link-state advertisement (LSA) packets for the neighbor, use the **neighbor database-filter all out** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to declare a router at address 172.16.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 172.16.3.4 priority 1 poll-interval 180
```

The following example illustrates a network with nonbroadcast:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-if)# ip address 172.16.3.10 255.255.255.0

RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-if)# network nonbroadcast
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 172.16.3.4 priority 1 poll-interval 180
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 172.16.3.5 cost 10 priority 1 poll-interval
180
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 172.16.3.6 cost 15 priority 1 poll-interval
180
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 172.16.3.7 priority 1 poll-interval 180
```

Related Commands

Command	Description
neighbor database-filter all out, on page 300	Filters all outgoing LSAs to an OSPF neighbor.
network (OSPF), on page 301	Configures the OSPF network type to a type other than the default for a given medium.
priority (OSPF), on page 316	Sets the router priority, which helps determine the designated router for this network.

neighbor database-filter all out

To filter all outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) neighbor, use the **neighbor database-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the neighbor, use the **no** form of this command.

neighbor *ip-address* **database-filter all out**
no neighbor *ip-address* **database-filter all out**

Syntax Description

ip-address	IP address of the neighbor to which outgoing LSAs are blocked.

Command Default

Instead of all outgoing LSAs being filtered to the neighbor, they are flooded to the neighbor.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **neighbor database-filter all out** command to filter all outgoing OSPF LSA packets during synchronization and flooding for point-to-multipoint neighbors on nonbroadcast networks. More neighbor options are available with the **neighbor** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to prevent flooding of OSPF LSAs from point-to-multipoint networks to the neighbor at IP address 10.2.3.4:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 10.2.3.4 database-filter all out
```

Related Commands

Command	Description
neighbor (OSPF), on page 298	Configures OSPF routers interconnecting to nonbroadcast networks.

network (OSPF)

To configure the Open Shortest Path First (OSPF) network type to a type other than the default for a given medium, use the **network** command in the appropriate mode. To return to the default value, use the **no** form of this command.

network {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}
no network

Syntax Description

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint	Sets the network type to point-to-multipoint.
non-broadcast	(Optional) Sets the point-to-multipoint network to be nonbroadcast. If you use this keyword, the **neighbor** command is required.
point-to-point	Sets the network type to point-to-point.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the network parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the network parameter specified for the process.

If this command is not specified at any level, then the OSPF network type is the default of the given medium.

POS interfaces default to point-to-point and

TenGigEthernet and HundredGigEthernet interfaces are default to broadcast.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **network** command to configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed network. However, there are other configurations where this assumption is not true; for example, a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected go through the router that has virtual circuits to both routers. You need not configure neighbors when using this command.

If this command is issued on an interface that does not allow it, this command is ignored.

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the OSPF network as a nonbroadcast network:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# network non-broadcast
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 172.16.3.4 priority 1 poll-interval 180
```

Related Commands

Command	Description
neighbor (OSPF), on page 298	Configures OSPF routers interconnecting to nonbroadcast networks.

nsf (OSPF)

To configure nonstop forwarding (NSF) for the Open Shortest Path First (OSPF) protocol, use the **nsf** command in the appropriate mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

nsf {**cisco** [**enforce global**] | **ietf** [**helper disable**]}
no nsf {**cisco** [**enforce global**] | **ietf** [**helper disable**]}

Syntax Description

cisco	Enables Cisco Nonstop Forwarding.
enforce global	(Optional) Cancels NSF restart when non-NSF network device neighbors are detected.
ietf	Enables Internet Engineering Task Force (IETF) graceful restart.
helper disable	(Optional) Disables router helper support.

Command Default

NSF is disabled.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The NSF feature allows for the forwarding of data packets to continue along known routes while routing protocol information (such as OSPF) is being restored following a switchover.

Use the **nsf** command if the router is expected to perform NSF during restart. To experience the full benefits of this feature, configure all neighboring routers with NSF.

When this command is used without the optional **cisco enforce global** keywords and non-NSF neighbors are detected, the NSF restart mechanism cancels on the interfaces of those neighbors and functions properly on others.

When this command is used with the optional **cisco enforce global** keywords and non-NSF neighbors are detected, NSF restart is canceled for the entire OSPF process.

IETF graceful restart provides an NSF mechanism to allow data traffic to flow seamlessly with no packet drops during the transient period when OSPF attempts to recover after a process restart or RP failover, within the guidelines of RFC 3623.

By default, neighbors in helper mode listen to both the NSF Cisco- and NSF IETF-type LSAs. The **nsf** command enables one type of mechanism that would undergo an RP failover or, anticipating an OSPF process

restart. If the **cisco** or **ietf** keyword is not entered, NSF is not enabled, irrespective of neighbors in listening mode for both NSF Cisco and NSF IETF.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to cancel NSF restart for the entire OSPF process if non-NSF neighbors are detected on any network interface during restart:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# nsf cisco enforce global
```

nsf flush-delay-time (OSPF)

To configure the maximum time allowed for nonstop forwarding (NSF) external route queries for the Open Shortest Path First (OSPF) protocol, use the **nsf flush-delay-time** command in the appropriate mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

nsf flush-delay-time *seconds*
no nsf flush-delay-time *seconds*

Syntax Description

seconds	Length of time (in seconds) allowed for NSF external route queries. Range is 1 to 3600 seconds.

Command Default

seconds : 300

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the maximum time for NSF to learn external routes for OSPF at 60 seconds:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# nsf flush-delay-time 60
```

nsf interval (OSPF)

To configure the minimum time between consecutive nonstop forwarding (NSF) restart attempts for the Open Shortest Path First (OSPF) protocol, use the **nsf interval** command in the appropriate mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

nsf interval *seconds*
no nsf interval *seconds*

Syntax Description

seconds	Length of time (in seconds) between consecutive restart attempts. Range is 90 to 3600 seconds.

Command Default

seconds : 90

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you use the **nsf interval** command, the OSPF process must be up for at least 90 seconds before OSPF attempts to perform an NSF restart.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the minimum time between consecutive NSF restart attempts at 120 seconds:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostnamer(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# nsf interval 120
```

nsf lifetime (OSPF)

To configure the maximum time that routes are held in the Routing Information Base (RIB) following an Open Shortest Path First (OSPF) process restart, use the **nsf lifetime** command in the appropriate mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

nsf lifetime *seconds*
no nsf lifetime *seconds*

Syntax Description

seconds	The length of time (in seconds) that routes are held in the RIB. Range is 90 to 3600 seconds.

Command Default

seconds : 95

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you use this command, the OSPF process must reconverge within the maximum length of time configured. If the convergence exceeds this length of time, routes are purged from RIB and nonstop forwarding (NSF) restart may fail.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the maximum lifetime for OSPF NSF at 120 seconds:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# nsf lifetime 120
```

nsr (OSPF)

To configure nonstop routing (NSR) for the Open Shortest Path First (OSPF) protocol, use the **nsr** command in OSPF router configuration mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

nsr
no nsr

Command Default

NSR is not defined.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The NSR feature allows an OSPF process on the active RP to synchronize all necessary data and states with the OSPF process on the standby RP. When the switchover happens, the OSPF process on the newly active RP has all the necessary data and states to continue running and does not require any help from its neighbors.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure NSR:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# nsr
```

nssa (OSPF)

To configure an area as a not-so-stubby area (NSSA), use the **nssa** command in area configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

nssa [**no-redistribution**] [**default-information-originate** [**metric** *metric-value*] [**metric-type** *type-value*]] [**no-summary**]
no nssa

Syntax Description

no-redistribution	(Optional) Imports routes only into the normal areas, but not into the NSSA area, by the **redistribute** command when the router is an NSSA Area Border Router (ABR).
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on an NSSA ABR or NSSA Autonomous System Boundary Router (ASBR).
metric *metric-value*	(Optional) Specifies the metric used for generating the default route. If you omit a value and do not specify a value using the **defaultmetric** command, the default metric value is 10. Range is 1 to 16777214.
metric-type *type-value*	(Optional) Specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: **1**—Type 1 external route **2**—Type 2 external route
no-summary	(Optional) Prevents an ABR from sending summary link advertisements into the NSSA.

Command Default

No NSSA area is defined.

Command Modes

Area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An NSSA does not flood Type 5 external LSAs from the core into the area, but can import autonomous system external routes in a limited fashion within the area.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure area 1 as an NSSA area:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 1
RP/0/RP0:hostname(config-ospf-ar)# nssa
```

ospf name-lookup

To configure the Open Shortest Path First (OSPF) protocol to look up Domain Name System (DNS) names, use the **ospf name-lookup** command in XR config mode. To disable this function, use the **no** form of this command.

ospf name-lookup
no ospf name-lookup

Command Default

Routers are displayed by router ID or neighbor ID.

Command Modes

XR config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **ospf name-lookup** command to easily identify a router when executing all OSPF **show** command displays. The router is displayed by name rather than by its router ID or neighbor ID.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure OSPF to identify a router by name:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ospf name-lookup
```

packet-size (OSPF)

To configure the size of Open Shortest Path First (OSPF) packets up to the size specified by the maximum transmission unit (MTU), use the **packet-size** command in the appropriate configuration mode. To disable this function and reestablish the default packet size, use the **no** form of this command.

packet-size *bytes*
no packet-size

Syntax Description

bytes	Size, in bytes. Range is 576 to 10000 bytes.

Command Default

If the command is not specified, the default packet size is either the interface IP MTU size (if that is lower than 9000 bytes) or 9000 bytes.

Command Modes

Router configuration

Area configuration

Interface configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **packet-size** command to customize the size of OSPF packets. The OSPF protocol compares the packet size and the MTU size and uses the lower packet size value.

If the command is not configured, the default packet size is equal to the interface IP MTU size (if that is lower than 9000 bytes) or 9000 bytes. For example, if the interface IP MTU size is 1500 bytes, OSPF uses packet size of 1500 bytes on the interface because the byte size is lower than 9000 bytes. If the interface IP MTU size is 9500 bytes, OSPF uses packet size of 9000 bytes on the interface because the byte size exceeds 9000 bytes. The interface IP MTU size depends on the interface and the platform. In most cases, the default interface IP MTU value will be lower than 9000 bytes.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the packet size on an interface:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-if)# packet-size 3500
```

passive (OSPF)

To suppress the sending of Open Shortest Path First (OSPF) protocol operation on an interface, use the **passive** command in the appropriate mode. To remove the passive configuration, use the **no** form of this command.

passive [{**disable** | **enable**}]
no passive

Syntax Description

disable	(Optional) Sends OSPF updates.
enable	(Optional) Disables sending OSPF updates.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the passive parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the passive parameter specified for the process.

If this command is not specified at any level, then the passive parameter is disabled and OSPF updates are sent on the interface.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

OSPF routing information is neither sent nor received through the specified interface. The interface appears as a stub network in the OSPF router (Type 1) link-state advertisement (LSA).

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows that Ten Gigabit Ethernet interface 0/6/0/2.10 reduces OSPF updates because passive mode is enabled; however, Gigabit Ethernet interface 0/6/0/6.11 receives normal OSPF traffic flow:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# passive
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/6.11
RP/0/RP0:hostname(config-ospf-ar-if)# end
```

priority (OSPF)

To set the router priority for an interface, which helps determine the designated router for an Open Shortest Path First (OSPF) link, use the **priority** command in the appropriate mode. To return to the default value, use the **no** form of this command.

priority *value*
no priority *value*

Syntax Description

value	8-bit unsigned integer indicating the router priority value. Range is 0 to 255.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the priority parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the priority parameter specified for the process.

If this command is not specified at any level, then the default priority is 1.

Command Modes

Interface configuration

Area configuration

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not point-to-point networks).

This priority value is used when you configure the Open Shortest Path First (OSPF) protocol for nonbroadcast networks using the **neighbor** command for OSPF.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows that priority is set through the **priority** and **neighbor** commands for Routers A and B and that the neighbor priority value must reflect that of the neighbor router:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-if)# ipv4 address 10.0.0.2 255.255.255.0
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# network non-broadcast
RP/0/RP0:hostname(config-ospf-ar-if)# priority 4
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 10.0.0.1 priority 6
```

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/3/0/2.10
RP/0/RP0:hostname(config-if)# ipv4 address 10.0.0.1 255.255.255.0
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# network non-broadcast
RP/0/RP0:hostname(config-ospf-ar-if)# priority 6
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 10.0.0.2 priority 4
```

Related Commands

Command	Description
neighbor (OSPF), on page 298	Configures OSPF routers interconnecting to nonbroadcast networks.
network (OSPF), on page 301	Configures the OSPF network type to a type other than the default for a given medium.

protocol shutdown

To disable an instance of the Open Shortest Path First (OSPF) protocol so that it cannot form an adjacency on any interface, use the **protocol shutdown** command in the router configuration mode. To reenable the OSPF protocol, use the **no** form of this command.

protocol shutdown
no protocol shutdown

Command Default

No default behavior or values

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **protocol shutdown** command to disable the OSPF protocol for a specific routing instance without removing any existing OSPF configuration parameters.

The OSPF protocol continues to run on the router and you can use the current OSPF configuration, but OSPF does not form any adjacencies on any interface.

This command is similar to performing the **no router ospf** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to disable the OSPF 1 instance:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospfv2 1
RP/0/RP0:hostname(config-ospf)# protocol shutdown
```

queue dispatch incoming

To limit the number of incoming packets (LSAUpdates, LSAcks, DBDs, LSRequests, and Hellos that trigger a change state) processed, use the **queue dispatch incoming** command in router configuration mode. To return to the system default value, use the **no** form of this command.

queue dispatch incoming *count*
no queue dispatch incoming

Syntax Description

count	Maximum number of continuous events processed. Range is 30 to 3000.

Command Default

The default incoming count is 300 packets (when the count is not configured).

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how limit the number of incoming packets processed to 500:

```
RP/0/RP0:hostname(config-ospf)# queue dispatch incoming 500
```

Use the show ospf message-queue, on page 369 command to see the queue dispatch values, peak lengths, and limits.

Related Commands

Command	Description
queue dispatch rate-limited-lsa, on page 321	Sets the maximum number of rate-limited link-state advertisements (LSAs) processed per run.
queue dispatch spf-lsa-limit, on page 323	Limits the number of summary or external Type 3 to Type 7 link-state advertisements (LSAs) processed per shortest path first (SPF) run.

Command	Description
queue limit, on page 325	Sets the high watermark for incoming priority events.
show ospf message-queue, on page 369	Displays the information about the queue dispatch values, peak lengths, and limits.

queue dispatch rate-limited-lsa

To set the maximum number of rate-limited link-state advertisement (LSA) (re-)originations processed per run, use the **queue dispatch rate-limited-lsa** command in router configuration mode. To return to the system default value, use the **no** form of this command.

queue dispatch rate-limited-lsa *count*
no queue dispatch rate-limited-lsa

Syntax Description

count	Maximum number of rate-limited LSAs processed per run. Range is 30 to 3000.

Command Default

The default number of rate-limited LSAs processed per run is 300 (when this count is not configured).

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set the maximum number of rate-limited LSA (re-)originations processed per run to 300:

```
RP/0/RP0:hostname(config-ospf)# queue dispatch rate-limited-lsa 300
```

Related Commands

Command	Description
queue dispatch incoming, on page 319	Limits the number of continuous incoming events processed.
queue dispatch spf-lsa-limit, on page 323	Limits the number of summary or external Type 3 to Type 7 link-state advertisements (LSAs) processed per shortest path first (SPF) run.
queue limit, on page 325	Sets the high watermark for incoming priority events.

Command	Description
show ospf message-queue, on page 369	Displays the information about the queue dispatch values, peak lengths, and limits.

queue dispatch spf-lsa-limit

To change the maximum number of Type 3-4 and Type 5-7 link-state advertisements (LSAs) processed per shortest path first (SPF) iteration within a single SPF run, use the **queue dispatch spf-lsa-limit** command in router configuration mode. To return to the system default value, use the **no** form of this command.

queue dispatch spf-lsa-limit *count*
no queue dispatch spf-lsa-limit

Syntax Description

count	Maximum number of continuous Type 3-4 and Type 5-7 LSAs processed per SPF in each scheduled iteration within a single SPF run. Range is 30 to 3000.

Command Default

The default number of Type 3-4 and Type 5-7 processed per run is 150 LSAs (when this command is not configured).

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to limit the number of continuous Type 3-4 and Type 5-7 LSAs processed by SPF per scheduling run, to 100:

```
RP/0/RP0:hostname(config-ospf)# queue dispatch spf-lsa-limit 100
```

Related Commands

Command	Description
queue dispatch incoming, on page 319	Limits the number of continuous incoming events processed.
queue dispatch rate-limited-lsa, on page 321	Sets the maximum number of rate-limited link-state advertisements (LSAs) processed per run
queue limit, on page 325	Sets the high watermark for incoming priority events.

Command	Description
show ospf message-queue, on page 369	Displays the information about the queue dispatch values, peak lengths, and limits.

queue limit

To set the high watermark for incoming events by priority, use the **queue limit** in router configuration mode. To return to the system default values, use the **no** form of this command.

queue limit {**high** | **medium** | **low**} *count*
no queue limit {**high** | **medium** | **low**}

Syntax Description

high	High watermark for incoming high-priority events (state-changing Hellos).
medium	High watermark for incoming medium-priority events (LSA ACK).
low	High watermark for incoming low-priority events (DBD/LSUpd/LSReq).
count	Maximum number of events per queue. Events are dropped when the priority queue size exceeds this value. Range is 1000 to 30000.

Command Default

High watermark: 9500 (when the corresponding configuration is not present).

Medium watermark: 9000 (when the corresponding configuration is not present).

Low watermark: 8000 (when the corresponding configuration is not present).

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Always keep the limits in the following order of priority:

Limit for High > Limit for Medium > Limit for Low

Task ID

Task ID	Operations
ospf	read, write

Examples

The following examples show how to set the maximum number of events per queue:

```
RP/0/RP0:hostname(config-ospf)# queue limit high 11000
RP/0/RP0:hostname(config-ospf)# queue limit medium 10000
RP/0/RP0:hostname(config-ospf)# queue limit low 9000
```

Related Commands

Command	Description
queue dispatch incoming, on page 319	Limits the number of continuous incoming events processed.
queue dispatch rate-limited-lsa, on page 321	Sets the maximum number of rate-limited link-state advertisements (LSAs) processed per run.
queue dispatch spf-lsa-limit, on page 323	Limits the number of summary or external Type 3 to Type 7 link-state advertisements (LSAs) processed per shortest path first (SPF) run.
show ospf message-queue, on page 369	Displays the information about the queue dispatch values, peak lengths, and limits.

range (OSPF)

To consolidate and summarize routes at an area boundary, use the **range** command in area configuration mode. To disable this function, use the **no** form of this command.

range *ip-address mask* [{**advertise** | **not-advertise**}]
no range *ip-address mask* [{**advertise** | **not-advertise**}]

Syntax Description

ip-address	IP address in four-part, dotted-decimal notation.
mask	IP address mask.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed and the component networks remain hidden from other networks.

Command Default

When this command is not specified for Area Border Routers (ABRs), routes at an area boundary are not consolidated or summarized.

Advertise is the default.

Command Modes

Area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **range** command only with Area Border Router (ABRs). Use the command to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This process is called *route summarization* .

Multiple range configurations specifying the **range** command can be configured. Thus, the OSPF protocol can summarize addresses for many different sets of address ranges.

The summarized route uses the maximum cost of the routes assumed in the range.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows area 36.0.0.0 consisting of interfaces whose IP addresses have "10.31.x.x" as the first two octets. The **range** command summarizes interfaces. Instead of advertising eight networks individually, the single route 10.31.0.0 255.255.0.0 is advertised:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/3/0/2
!
RP/0/RP0:hostname(config-ospf)# area 36.0.0.0
RP/0/RP0:hostname(config-ospf-ar)# range 10.31.0.0 255.255.0.0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/1/0/1
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/1/0/2
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/1/0/3
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/2/0/0
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/2/0/1
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/2/0/2
RP/0/RP0:hostname(config-ospf-ar-if)# interface TenGigE0/2/0/3
RP/0/RP0:hostname(config-ospf-ar-if)# end
```

Related Commands

Command	Description
summary-prefix (OSPF), on page 405	Creates aggregate addresses for routes being redistributed from another routing protocol into the OSPF protocol.

redistribute (OSPF)

To redistribute routes from one routing domain into Open Shortest Path First (OSPF), use the **redistribute** command in the appropriate mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

Border Gateway Protocol (BGP)
redistribute bgp *process-id* [**preserve-med**] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute bgp *process-id* [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Local Interface Routes
redistribute connected [**instance** *instance-name*] [**instance IPCP**][**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute connected [**instance** *instance-name*] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Directed-attached gateway redundancy (DAGR)
redistribute dagr [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute dagr [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Enhanced Interior Gateway Routing Protocol (EIGRP)
redistribute eigrp *process-id* [**match** {**external** [{**1** | **2**}] | **internal**}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute eigrp *process-id* [**match** {**external** [{**1** | **2**}] | **internal**}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Intermediate System-to-Intermediate System (IS-IS)
redistribute isis *process-id* [{**level-1** | **level-2** | **level-1-2**}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute isis *process-id* [{**level-1** | **level-2** | **level-1-2**}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Open Shortest Path First (OSPF)
redistribute ospf *process-id* [**match** {**external** [{**1** | **2**}] | **internal** | **nssa-external** [{**1** | **2**}]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute ospf *process-id* [**match** {**external** [{**1** | **2**}] | **internal** | **nssa-external** [{**1** | **2**}]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Routing Information Protocol (RIP)
redistribute rip [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute rip [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

IP Static Routes
redistribute static [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
no redistribute static [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Syntax Description

bgp	Distributes routes from the BGP protocol.
process-id	For the **bgp** keyword, an autonomous system number has the following ranges: • Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. • Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. • Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535. For the **isis** keyword, an IS-IS instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string. For the **ospf** keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
preserve-med	(Optional) Preserves the Multi Exit Discriminator (MED) of BGP routes.
metric *metric-value*	(Optional) Specifies the metric used for the redistributed route. Range is 1 to 16777214. Use a value consistent with the source protocol.
metric-type { **1** | **2** }	(Optional) Specifies the external link type associated with the route advertised into the OSPF routing domain. It can be one of two values: • **1** —Type 1 external route • **2** —Type 2 external route
tag *tag-value*	(Optional) Specifies the value attached to each external route. This value is not used by the OSPF protocol itself, but is carried in the external LSAs. Range is 0 to 4294967295.
route-policy *policy-name*	(Optional) Specifies the identifier of a configured policy. A policy is used to filter the importation of routes from this source routing protocol to OSPF.
connected	Distributes routes that are established automatically by virtue of having enabled IP on an interface.
instance	Connected instance.
instance-name	Name of the connected instance.
instance IPCP	Distributes routes from IPCP protocols.
eigrp	Distributes routes from the EIGRP protocol.
isis	Distributes routes from the IS-IS protocol.

level-1	(Optional) Redistributes Level 1 routes into other IP routing protocols independently.
l **evel-1-2**	(Optional) Distributes both Level 1 and Level 2 routes into other IP routing protocols.
level-2	(Optional) Distributes Level 2 routes into other IP routing protocols independently.
ospf	Distributes routes from the OSPF protocol.
match { **internal** | **external [1** | **2**] | **nssa-external** [**1** | **2]** }	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one or more of the following: • **internal** —Routes that are internal to a specific autonomous system (intra- and inter-area OSPF routes). • **external** [**1 | 2**]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • **nssa-external** [**1 | 2**]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 not-so-stubby area (NSSA) external routes. For the **external** and **nssa-external** options, if a type is not specified, then both Type 1 and Type 2 are assumed. If no match is specified, the default is no filtering.
rip	Distributes routes from the RIP protocol.
static	Distributes IP static routes.
dagr	Distributes routes from the directed-attached gateway redundancy (DAGR).

Command Default

Route redistribution is disabled.

metric *metric-value:* Default is 20 for routes from all protocols except BGP routes, for which the default is 1.

metric-type : Type 2 external route.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note When redistributing routes (into OSPF) using both command keywords for setting or matching of attributes and a route policy, the routes are run through the route policy first, followed by the keyword matching and setting.

Redistributed routing information should always be filtered by the **policy** *policy-name* keyword and argument. This filtering ensures that only those routes intended by the administrator are redistributed into OSPF.

Whenever you use the **redistribute** or default-information originate (OSPF), on page 251 command to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the OSPF routing domain.

When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

When routes are redistributed into OSPF and no metric is specified with the **metric** keyword, OSPF uses 20 as the default metric for routes from all protocols except BGP routes, which get a metric of 1.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to cause BGP routes to be redistributed into an OSPF domain:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 110
RP/0/RP0:hostname(config-ospf)# redistribute bgp 100
```

The following example shows how to redistribute the specified IS-IS process routes into an OSPF domain. The IS-IS routes are redistributed with a metric of 100.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# redistribute isis 108 metric 100
```

In the following example, network 10.0.0.0 appears as an external link-state advertisement (LSA) in OSPF 1:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-if)# ip address 10.0.0.0 255.0.0.0
!
RP/0/RP0:hostname(config)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config)# ip address 10.99.0.0 255.0.0.0
!
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# redistribute ospf 2
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
!
RP/0/RP0:hostname(config)# router ospf 2
```

```
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Related Commands

Command	Description
default-information originate (OSPF), on page 251	Generates a default external route into an OSPF routing domain.

retransmit-interval (OSPF)

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First (OSPF) interface, use the **retransmit-interval** command in the appropriate mode. To return to the default value, use the **no** form of this command.

retransmit-interval *seconds*
no retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. Range is 1 to 65535 seconds.

Command Default

If this command is not specified in interface configuration mode, then the interface adopts the retransmit interval parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the retransmit interval parameter specified for the process.

If this command is not specified at any level, then the default retransmit interval is 5 seconds.

Command Modes

Interface configuration

Area configuration

Router configuration

Virtual-link configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it resends the LSA.

The setting of this parameter should be conservative, or needless retransmission results. The value should be larger for serial lines and virtual links.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set the retransmit interval value to 8 seconds in interface configuration mode:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
RP/0/RP0:hostname(config-ospf-ar-if)# retransmit-interval 8
```

router-id (OSPF)

To configure a router ID for the Open Shortest Path First (OSPF) process, use the **router-id** command in the appropriate mode. To cause the software to use the default method of determining the router ID, use the **no** form of this command after clearing or restarting the OSPF process.

router-id router-id
no router-id router-id

Syntax Description

router-id	32-bit router ID value specified in four-part, dotted-decimal notation.

Command Default

If this command is not configured, the router ID is the highest IP version 4 (IPv4) address for an interface on the router, with any loopback interface taking precedence.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

It is good practice to use the **router-id** command to explicitly specify a unique 32-bit numeric value for the router ID. This action ensures that OSPF can function regardless of the interface address configuration. Clear the OSPF process using the **clear ospf process** command or restart the OSPF process for the **no router-id** command to take effect.

OSPF attempts to obtain a router ID in the following ways (in order of preference):

1. By default, when the OSPF process initializes, it checks if there is a router-id in the checkpointing database.
2. The 32-bit numeric value specified by the OSPF **router-id** command in router configuration mode. (This value can be any 32-bit value. It is not restricted to the IPv4 addresses assigned to interfaces on this router, and need not be a routable IPv4 address.)
3. The ITAL selected router-id.
4. The primary IPv4 address of an interface over which this OSPF process is running. The first interface address in the OSPF interface is selected.

Note Unlike OSPF version 3, OSPF version 2 is guaranteed to have at least one interface with an IPv4 address configured.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to assign the IP address of 172.20.10.10 to the OSPF process 109:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
RP/0/RP0:hostname(config-ospf)# router-id 172.20.10.10
```

Related Commands

Command	Description
clear ospf process, on page 234	Resets an OSPF router process without stopping and restarting it.
ipv4 address	Sets a primary IPv4 address for an interface.

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in XR config mode. To terminate an OSPF routing process, use the **no** form of this command.

router ospf *process-name*
no router ospf *process-name*

Syntax Description

process-name	Name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters without spaces.

Command Default

No OSPF routing process is defined.

Command Modes

XR config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can specify multiple OSPF routing processes in each router. Up to 10 processes can be configured. The recommendation is not to exceed 4 OSPF processes.

All OSPF configuration commands must be configured under an OSPF routing process. For example, two of these commands are the **default-metric** command and the **router-id** command.

Task ID

Task ID	Operations
ospf	read, write
rib	read, write

Examples

The following example shows how to instantiate an OSPF routing process called 109:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 109
```

Related Commands

Command	Description
area (OSPF), on page 225	Configures an OSPF area.
default-metric (OSPF), on page 253	Sets default metric values for routes redistributed from another protocol into the OSPF protocol.
interface (OSPF), on page 273	Defines the interfaces on which the OSPF protocol runs.
router-id (OSPF), on page 336	Configures a router ID for the OSPF process.

show ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ospf** command in exec mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [**summary**]

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved values of the *vrf-name* argument.
summary	(Optional) Displays OSPF summary information.

Command Default

IPv4 and unicast address prefixes

Command Modes

exec

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show ospf** command to provide basic information about the OSPF processes running on the router. Additional options provide in-depth information.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf** command:

```
RP/0/RP0:hostname#show ospf

Routing Process "ospf 1" with ID 1.1.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
```

```
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Minimum LSA interval 5000 msecs. Minimum LSA arrival 1 secs
Maximum number of configured interfaces 255
Number of external LSA 0. Checksum Sum 00000000
Number of opaque AS LSA 0. Checksum Sum 00000000
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 2. 2 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled
   Area BACKBONE(0) (Inactive)
       Number of interfaces in this area is 2
       SPF algorithm executed 8 times
       Number of LSA 2. Checksum Sum 0x01ba83
       Number of opaque link LSA 0. Checksum Sum 00000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
   Area 1
       Number of interfaces in this area is 1
       SPF algorithm executed 9 times
       Number of LSA 2. Checksum Sum 0x0153ea
       Number of opaque link LSA 0. Checksum Sum 00000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

This table describes the significant fields shown in the display.

Table 2: show ospf Field Descriptions

Field	Description
Routing Process “ospf 201” with ID 172.22.110.200	OSPF process name.
Supports only	Number of types of service supported (Type 0 only).
It is	Types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
SPF schedule delay	Delay time of SPF calculations.
Minimum LSA interval	Minimum interval between LSAs.
Minimum LSA arrival	Minimum elapsed time between accepting an update for the same link-state advertisement (LSA).
external LSA	Total number of Type 5 LSAs in the LSDB.
opaque LSA	Total number of Type 10 LSAs in the LSDB.
DCbitless...AS LSA	Total number of Demand Circuit Type 5 and Type 11 LSAs.

Field	Description
DoNotAge...AS LSA	Total number of Type 5 and Type 11 LSAs with the DoNotAge bit set.
Number of areas	Number of areas in router, area addresses, and so on.
Area BACKBONE	Backbone is area 0.

This sample output from the **show ospf vrf** *vrf_name* command displays the VRF Lite status:

```
RP/0/RP0:hostname#show ospf vrf vrf1

 VRF vrf1 in Routing Process "ospf 100" with ID 1.1.1.1
 NSR (Non-stop routing) is Disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 VRF Lite is enabled
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 50 msecs
 Minimum hold time between two consecutive SPFs 200 msecs
 Maximum wait time between two consecutive SPFs 5000 msecs
 Initial LSA throttle delay 50 msecs
 Minimum hold time for LSA throttle 200 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA interval 200 msecs. Minimum LSA arrival 100 msecs
 LSA refresh interval 1800 seconds
 Flood pacing interval 33 msecs. Retransmission pacing interval 66 msecs
 Adjacency stagger enabled; initial (per area): 2, maximum: 64
    Number of neighbors forming: 0, 2 full
 Maximum number of configured interfaces 1024
 Number of external LSA 0. Checksum Sum 00000000
 Number of opaque AS LSA 0. Checksum Sum 00000000
 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 2. 2 normal 0 stub 0 nssa
 External flood list length 0
 SNMP trap is disabled
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        SPF algorithm executed 4 times
        Number of LSA 16.  Checksum Sum 0x071c6a
        Number of opaque link LSA 0.  Checksum Sum 00000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
        Number of LFA enabled interfaces 0, LFA revision 0
        Number of Per Prefix LFA enabled interfaces 0
        Number of neighbors forming in staggered mode 0, 1 full
    Area 1
        Number of interfaces in this area is 4
        SPF algorithm executed 5 times
        Number of LSA 14.  Checksum Sum 0x066d93
        Number of opaque link LSA 0.  Checksum Sum 00000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
        Number of LFA enabled interfaces 0, LFA revision 0
        Number of Per Prefix LFA enabled interfaces 0
```

```
Number of neighbors forming in staggered mode 0, 1 full
```

show ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ospf border-routers** command in EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] **border-routers** [*router-id*]

Syntax Description

process-name	(Optional) OSPF process name. If this argument is included, only information for the specified routing process is included.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved vrf-names.
router-id	(Optional) Router ID associated with the border router. The value of the *router-id* argument can be any 32-bit router ID value specified in four-part, dotted-decimal notation. No default exists.

Command Default

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show ospf border-routers** command to list all OSPF border routers visible to the specified processes and to ascertain the OSPF topology of the router.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf border-routers** command:

```
RP/0/RP0:hostname# show ospf border-routers

OSPF 1 Internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.31.97.53 [1] via 172.16.1.53, TenGigE0/6/0/2.10, ABR/ASBR , Area 0, SPF 3
```

This table describes the significant fields shown in the display.

Table 3: show ospf border-routers Field Descriptions

Field	Description
i	Type of this route; i indicates an intra-area route, I an interarea route.
172.31.97.53	Router ID of destination.
[1]	Cost of using this route.
172.16.1.53	Next-Next hop toward the destination.
TenGigE0/6/0/2.10	Packets destined for 172.16.1.53 are sent over Ten Gigabit Ethernet interface 0/6/0/2.10.
ABR/ASBR	Router type of the destination; it is either an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) or both.
Area 0	Area ID of the area from which this route is learned.
SPF 3	Internal number of the shortest path first (SPF) calculation that installs this route.

show ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ospf database** command in EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database**
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**adv-router** *ip-address*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**asbr-summary**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**internal**] [**self-originate**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**database-summary**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**external**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**external**] [*link-state-id*] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**external**] [*link-state-id*] [**internal**] [**self-originate**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**network**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**network**] [*link-state-id*] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**network**] [*link-state-id*] [**internal**] [**self-originate**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**nssa-external**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**internal**] [**self-originate**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-area**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-area**] [*link-state-id*] [**internal**] [**adv-router**] [*ip-address*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-area**] [*link-state-id*] [**internal**] [**self-originate**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-as**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-as**] [*link-state-id*] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-as**] [*link-state-id*] [**internal**] [**self-originate**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-link**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-link**] [*link-state-id*] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**opaque-link**] [*link-state-id*] [**internal**] [**self-originate**]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**router**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**router**] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**router**] [**internal**] [**self-originate**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**self-originate**]

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**summary**] [*link-state-id*]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**summary**] [*link-state-id*] [**internal**] [**adv-router** [*ip-address*]]
show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **database** [**summary**] [*link-state-id*] [**internal**] [**self-originate**] [*link-state-id*]

Syntax Description

process-name	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.
vrf	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF. The *vrf-name* argument can be specified as an arbitrary string. The strings “default” and “all” are reserved VRF names.
all	(Optional) Specifies all OSPF VRF instances.
area-id	(Optional) Area number used to define the particular area.
adv-router *ip-address*	(Optional) Displays all LSAs of the specified router.
asbr-summary	(Optional) Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.
link-state-id	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the link-state type of the advertisement. It must be entered in the form of an IP address. When the link-state advertisement (LSA) is describing a network, the *link-state-id* can take one of two forms: • The network IP address (as in Type 3 summary link advertisements and in autonomous system external link advertisements). • A derived address obtained from the link-state ID. **Note** Masking the link-state ID of a network link advertisement with the subnet mask of the network yields the IP address of the network. When the LSA is describing a router, the link-state ID is always the OSPF router ID of the described router. When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link-state ID is set to Default Destination (0.0.0.0).
internal	(Optional) Displays internal LSA information.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
database-summary	(Optional) Displays how many of each type of LSA for each area there are in the database and the total.
external	(Optional) Displays information only about the external LSAs.
network	(Optional) Displays information only about the network LSAs.

nssa-external	(Optional) Displays information only about the not-so-stubby area (NSSA) external LSAs.
opaque-area	(Optional) Displays information about the opaque Type 10 LSAs. Type 10 denotes an area-local scope. Refer to RFC 2370 for more information on the opaque LSA options.
opaque-as	(Optional) Displays information about the opaque Type 11 LSAs. Type 11 denotes that the LSA is flooded throughout the autonomous system.
opaque-link	(Optional) Displays information about the opaque Type 9 LSAs. Type 9 denotes a link-local scope.
router	(Optional) Displays information only about the router LSAs.
summary	(Optional) Displays information only about the summary LSAs.

Command Default

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The various forms of the **show ospf database** command deliver information about different OSPF link-state advertisements. This command can be used to examine the link-state database (LSD) and its contents. Each router participating in an area having identical database entries pertaining to that area (with the exception of LSAs that are being flooded). Numerous options (such as **network** and **router**) are used to display portions of the database.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf database** command when no arguments or keywords are used:

```
RP/0/RP0:hostname# show ospf database

OSPF Router with ID (172.20.1.11) (Process ID 1)

                Router Link States (Area 0)

 Link ID         ADV Router      Age         Seq#       Checksum Link count
 172.20.1.8       172.20.1.8       1381      0x8000010D    0xEF60   2
```

```
172.20.1.11      172.20.1.11      1460      0x800002FE    0xEB3D   4
172.20.1.12      172.20.1.12      2027      0x80000090    0x875D   3
172.20.1.27      172.20.1.27      1323      0x800001D6    0x12CC   3

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.22.1.27      172.20.1.27      1323      0x8000005B    0xA8EE
172.22.1.11      172.20.1.11      1461      0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Opaque ID
10.0.0.0         172.20.1.11      1461      0x800002C8    0x8483     0
10.0.0.0         172.20.1.12      2027      0x80000080    0xF858     0
10.0.0.0         172.20.1.27      1323      0x800001BC    0x919B     0
10.0.0.1         172.20.1.11      1461      0x8000005E    0x5B43     1
```

This table describes the significant fields shown in the display.

Table 4: show ospf database Field Descriptions

Field	Description
Link ID	Router ID number.
ADV Router	ID of the advertising router.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.
Link count	Number of interfaces detected for the router.
Opaque ID	Opaque LSA ID number.

The following is sample output from the **show ospf database** command with the **asbr-summary** keyword:

```
RP/0/RP0:hostname# show ospf database asbr-summary

OSPF Router with ID (192.168.0.1) (Process ID 300)

Summary ASB Link States (Area 0.0.0.0)

  LS age: 1463
  Options: (No TOS-capability)
  LS Type: Summary Links (AS Boundary Router)
  Link State ID: 172.17.245.1 (AS Boundary Router address)
  Advertising Router: 172.17.241.5
  LS Seq Number: 80000072
  Checksum: 0x3548
  Length: 28
  Network Mask: /0
 TOS: 0  Metric: 1
```

This table describes the significant fields shown in the display.

Table 5: show ospf database asbr-summary Field Descriptions

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (ASBR).
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSAs.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

The following is sample output from the **show ospf database** command with the **external** keyword:

```
RP/0/RP0:hostname# show ospf database external

OSPF Router with ID (192.168.0.1) (Process ID 300)

                  Type-5 AS External Link States

  LS age: 280
  Options: (No TOS-capability)
  LS Type: AS External Link
  Link State ID: 172.17.0.0 (External Network Number)
  Advertising Router: 172.17.70.6
  LS Seq Number: 80000AFD
  Checksum: 0xC3A
  Length: 36
  Network Mask: 255.255.0.0
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 1
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

This table describes the significant fields shown in the display.

Table 6: show ospf database external Field Descriptions

Field	Description
OSPF Router with Router ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (external network number).
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Network Mask	Network mask implemented.
Metric Type	External type.
TOS	Type of service.
Metric	Link-state metric.
Forward Address	Forwarding address. Data traffic for the advertised destination is forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic is forwarded instead to the originator of the advertisement.
External Route Tag	External route tag, a 32-bit field attached to each external route. This tag is not used by the OSPF protocol itself.

The following is sample output from the **show ospf database** command with the **network** keyword:

```
RP/0/RP0:hostname# show ospf database network

 OSPF Router with ID (192.168.0.1) (Process ID 300)

Net Link States (Area 0.0.0.0)

  LS age: 1367
  Options: (No TOS-capability)
  LS Type: Network Links
  Link State ID: 172.23.1.3 (address of Designated Router)
  Advertising Router: 192.168.0.1
```

```
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: /24
      Attached Router: 192.168.0.1
      Attached Router: 172.23.241.5
      Attached Router: 172.23.1.1
      Attached Router: 172.23.54.5
      Attached Router: 172.23.1.5
```

This table describes the significant fields shown in the display.

Table 7: show ospf database network Field Descriptions

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID of the designated router.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Network Mask	Network mask implemented.
Attached Router	List of routers attached to the network, by IP address.

The following is sample output, carrying Multiprotocol Label Switching traffic engineering (MPLS TE) specification information, from the **show ospf database** command with the **opaque-area** keyword and a *link-state-id* of adv-router:

```
RP/0/RP0:hostname# show ospf database opaque-area adv-router 172.20.1.12

  OSPF Router with ID (172.20.1.11) (Process ID 1)

                Type-10 Opaque Link Area Link States (Area 0)

   LS age: 224
   Options: (No TOS-capability, DC)
   LS Type: Opaque Area Link
   Link State ID: 1.0.0.0
   Opaque Type: 1
   Opaque ID: 0
   Advertising Router: 172.20.1.12
```

```
  LS Seq Number: 80000081
  Checksum: 0xF659
  Length: 132
  Fragment number : 0

    MPLS TE router ID : 172.20.1.12

    Link connected to Point-to-Point network
      Link ID : 172.20.1.11
      Interface Address : 172.21.1.12
      Neighbor Address : 172.21.1.11
      Admin Metric : 10
      Maximum bandwidth : 193000
      Maximum reservable bandwidth : 125000
      Number of Priority : 8
      Priority 0 : 125000      Priority 1 : 125000
      Priority 2 : 125000      Priority 3 : 125000
      Priority 4 : 125000      Priority 5 : 125000
      Priority 6 : 125000      Priority 7 : 100000
      Affinity Bit : 0x0

    Number of Links : 1
```

The following is the sample output from the **show ospf database opaque-area** command displaying the extended link LSA information.

```
RP/0/RP0:hostname# show ospf database opaque-area 4.0.0.0
LS age: 361
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 8.0.0.40
  Opaque Type: 8
  Opaque ID: 40
  Advertising Router: 100.0.0.3
  LS Seq Number: 8000012e
Checksum: 0xeab4
  Length: 92

    Extended Link TLV: Length: 68
      Link-type : 2
      Link ID   : 100.0.9.4
      Link Data : 100.0.9.3

     LAN Adj sub-TLV: Length: 16
       Flags      : 0x0
       MTID       : 0
       Weight     : 0
       Neighbor ID: 100.0.0.1

       SID/Label sub-TLV: Length: 3
          SID       : 24001

     LAN Adj sub-TLV: Length: 16
       Flags      : 0x0
       MTID       : 0
       Weight     : 0
       Neighbor ID: 100.0.0.2

       SID/Label sub-TLV: Length: 3
          SID       : 24000
```

```
  Adj sub-TLV: Length: 12
     Flags     : 0x0
     MTID      : 0
     Weight    : 0

    SID/Label sub-TLV: Length: 3
       SID       : 24002
```

The following is sample output from the **show ospf database** command that displays a Type 10, Router Information LSA:

```
RP/0/RP0:hostname# show ospf database opaque-area 4.0.0.0

            OSPF Router with ID (3.3.3.3) (Process ID orange)

                Type-10 Opaque Link Area Link States (Area 0)

  LS age: 105
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 4.0.0.0
  Opaque Type: 4
  Opaque ID: 0
  Advertising Router: 3.3.3.3
  LS Seq Number: 80000052
  Checksum: 0x34e2
  Length: 52
  Fragment number: 0

    Router Information TLV: Length: 4
    Capabilities:
      Graceful Restart Helper Capable
      Traffic Engineering enabled area
      All capability bits: 0x50000000

    PCE Discovery TLV: Length: 20
      IPv4 Address: 3.3.3.3
      PCE Scope: 0x20000000
      Compute Capabilities:
      Inter-area default (Rd-bit)
      Compute Preferences:
      Intra-area: 0  Inter-area:  0
      Inter-AS:   0  Inter-layer: 0
```

This table describes the significant fields shown in the display.

Table 8: show ospf database opaque-area Field Descriptions

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.

Field	Description
Link State ID	Link-state ID.
Opaque Type	Opaque link-state type.
Opaque ID	Opaque ID number.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Fragment number	Arbitrary value used to maintain multiple traffic engineering LSAs.
Link ID	Link ID number.
Interface Address	ID address of the interface.
Neighbor Address	IP address of the neighbor.
Admin Metric	Administrative metric value used by MPLS TE.
Maximum bandwidth	Specifies maximum bandwidth (in kbps).
Maximum reservable bandwidth	Specifies maximum reservable bandwidth (in kbps).
Number of Priority	Priority number.
Affinity Bit	Used by MPLS TE.
Router Information TLV	Router capabilities are advertised in this TLV.
Capabilities	Some router capabilities include stub router, traffic engineering, graceful restart, and graceful restart helper.
PCE Discovery TLV	PCE address and capability information is advertised in this TLV.
IPv4 Address	Configured PCE IPv4 address.
PCE Scope	Computation capabilities of the PCE.
Compute Capabilities	Compute capabilities and preferences of the PCE.
Inter-area default (RD-bit)	PCE compute capabilities such as intra-area, inter-area, inter-area default, inter-AS, inter-AS default and inter-layer.
Compute Preferences	Order or preference of path computation that includes intra-area, inter-area, inter-AS, and inter-layer preferences.

The following is sample output from the **show ospf database** command with the **router** keyword:

```
RP/0/RP0:hostname# show ospf database router

OSPF Router with ID (192.168.0.1) (Process ID 300)

Router Link States (Area 0.0.0.0)

  LS age: 1176
  Options: (No TOS-capability)
  LS Type: Router Links
  Link State ID: 172.23.21.6
  Advertising Router: 172.23.21.6
  LS Seq Number: 80002CF6
  Checksum: 0x73B7
  Length: 120
  AS Boundary Router
  Number of Links: 8

 Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 172.23.21.5
(Link Data) Router Interface address: 172.23.21.6
 Number of TOS metrics: 0
  TOS 0 Metrics: 2
```

This table describes the significant fields shown in the display.

Table 9: show ospf database router Field Descriptions

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
AS Boundary Router	Definition of router type.
Number of Links	Number of active links.
Link ID	Link type.
Link Data	Router interface address.

Field	Description
TOS	Type of service metric (Type 0 only).

The following is sample output from **show ospf database** command with the **summary** keyword:

```
RP/0/RP0:hostname# show ospf database summary

       OSPF Router with ID (192.168.0.1) (Process ID 300)

 Summary Net Link States (Area 0.0.0.0)

  LS age: 1401
  Options: (No TOS-capability)
  LS Type: Summary Links (Network)
  Link State ID: 172.23.240.0 (Summary Network Number)
  Advertising Router: 172.23.241.5
  LS Seq Number: 80000072
  Checksum: 0x84FF
  Length: 28
  Network Mask: /24
     TOS: 0  Metric: 1
```

This table describes the significant fields shown in the display.

Table 10: show ospf database summary Field Descriptions

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (summary network number).
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

The following is sample output from **show ospf database** command with the **database-summary** keyword:

```
RP/0/RP0:hostname# show ospf database database-summary

          OSPF Router with ID (172.19.65.21) (Process ID 1)

Area 0 database summary
  LSA Type      Count    Delete   Maxage
  Router        2        0        0
  Network       1        0        0
  Summary Net   2        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Subtotal      5        0        0

Process 1 database summary
  LSA Type      Count    Delete   Maxage
  Router        2        0        0
  Network       1        0        0
  Summary Net   2        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Type-5 Ext    2        0        0
  Opaque AS     0        0        0
  Total         7        0        0
```

This table describes the significant fields shown in the display.

Table 11: show ospf database database-summary Field Descriptions

Field	Description
LSA Type	Link-state type.
Count	Number of advertisements in that area for each link-state type.
Delete	Number of LSAs that are marked “Deleted” in that area.
Maxage	Number of LSAs that are marked “Maxaged” in that area.

show ospf flood-list

To display a list of Open Shortest Path First (OSPF) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ospf flood-list** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **flood-list** [*type interface-path-id*]

Syntax Description

process-name	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.
vrf	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.
all	(Optional) Specifies all OSPF VRF instances.
area-id	(Optional) Area number used to define the particular area.
type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

All interfaces

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show ospf flood-list** command to display LSAs in flood queue and queue length.

Flood list information is transient and normally the flood lists are empty.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf flood-list** command for interface TenGigE0/3/0/5.20:

```
RP/0/RP0:hostname# show ospf flood-list TenGigE0/3/0/5.20

 Interface TenGigE0/3/0/5.20, Queue length 20
 Link state retransmission due in 12 msec
 Displaying 6 entries from flood list:

 Type  LS ID           ADV RTR         Seq NO      Age    Checksum
    5  10.2.195.0       200.0.0.163     0x80000009  0      0xFB61
    5  10.1.192.0       200.0.0.163     0x80000009  0      0x2938
    5  10.2.194.0       200.0.0.163     0x80000009  0      0x757
    5  10.1.193.0       200.0.0.163     0x80000009  0      0x1E42
    5  10.2.193.0       200.0.0.163     0x80000009  0      0x124D
    5  10.1.194.0       200.0.0.163     0x80000009  0      0x134C
```

This table describes the significant fields shown in the display.

Table 12: show ospf flood-list Field Descriptions

Field	Description
TenGigE0/3/0/5.20	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time (in milliseconds) before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of the advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of the LSA (in seconds).
Checksum	Checksum of the LSA.

show ospf interface

To display Open Shortest Path First (OSPF) interface information, use the **show ospf interface** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **interface** [**brief**] [*type interface-path-id*]

Syntax Description

process-name	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.
vrf	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.
all	(Optional) Specifies all OSPF VRF instances.
area-id	(Optional) Area number used to define the particular area.
brief	(Optional) Displays brief interface information.
type	Interface type.
interface-path-id	Physical interface or virtual interface. Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

All interfaces

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf interface** command which includes the topology independent loop free alternates (TI LFA) related information:

```
 RP/0/RP0:hostname# show ospf interface

  TenGigE0/3/0/5.20 is up, line protocol is up
  Internet Address 1.2.2.1/24, Area 0
  Process ID 1, Router ID 0.0.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1, MTU 1500, MaxPktSz 1500
  Designated Router (ID) 0.0.0.2, Interface address 1.2.2.2
  Backup Designated router (ID) 0.0.0.1, Interface address 1.2.2.
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02:857
  Index 2/2, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  LS Ack List: current length 0, high water mark 6
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 0.0.0.2  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 0
Fast-reroute type Per-prefix
    Topology Independent LFA enabled
```

This table describes the significant fields shown in the display.

Table 13: show ospf interface Field Descriptions

Field	Description
TenGigE0/3/0/5.20	Status of the physical link.
line protocol	Operational status of the protocol.
Internet Address	Interface IP address, subnet mask, and area address.
Process ID	OSPF process ID, router ID, network type, and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until next hello packet is sent over this interface.
Index	Area and autonomous system flood indexes.
Next 0 (0) /0 (0)	Next area and autonomous system flood information, data pointer, and index.
Last flood scan length	Length of last flood scan.
Last flood scan time	Time (in milliseconds) of last flood scan.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.
Suppress hello	Count of neighbors suppressing hello messages.
Multi-area interface	Multiple area interface information for the primary interface, such as count and area/neighbor locations.

This table describes the significant fields shown in the display.

Table 14: show ospf interface Field Descriptions

Field	Description
POS	Status of the physical link.
line protocol	Operational status of the protocol.
Internet Address	Interface IP address, subnet mask, and area address.
Process ID	OSPF process ID, router ID, network type, and link-state cost.
LDP Sync Enabled, Sync Status	LDP Sync configuration state and operational status. Displayed only when the OSPF process is configured for MPLS LDP Sync.
Transmit Delay	Transmit delay, interface state, and router priority.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until next hello packet is sent over this interface.
Index 1/1	Area and autonomous system flood indexes.
Next 0x0(0)	Next area and autonomous system flood information, data pointer, and index.
Last flood scan length	Length of last flood scan.
Last flood scan time	Time (in milliseconds) of last flood scan.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.
Suppress hello	Count of neighbors suppressing hello messages.
Multi-area interface	Multiple area interface information for the primary interface, such as count and area/neighbor location.

show ospf mpls traffic-eng

To display information about the links and fragments available on the local router for traffic engineering, use the **show ospf mpls traffic-eng** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] [*type interface-path-id*] **mpls traffic-eng** {**link** | **fragment**}

Syntax Description

process-name	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.
area-id	(Optional) Area number used to define the particular area.
type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
link	Provides detailed information about the links over which traffic engineering is supported on the local router.
fragment	Provides detailed information about the traffic engineering fragments on the local router.

Command Default

All links or fragments

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf mpls traffic-eng** command when the **link** keyword is specified:

```
RP/0/RP0:hostname# show ospf mpls traffic-eng link

            OSPF Router with ID (10.10.10.10) (Process ID 1)

  Area 0 has 2 MPLS TE links. Area instance is 67441.

  Links in hash bucket 3.
    Link is associated with fragment 1. Link instance is 67441
      Link connected to Point-to-Point network
      Link ID : 10.10.10.8
      Interface Address : 10.10.10.2
      Neighbor Address : 10.10.10.3
      Admin Metric : 0
      Maximum bandwidth : 19440000
      Maximum global pool reservable bandwidth : 25000000
      Maximum sub pool reservable bandwidth    : 3125000
      Number of Priority : 8
      Global pool unreserved BW
      Priority 0 :   25000000  Priority 1 :   25000000
      Priority 2 :   25000000  Priority 3 :   25000000
      Priority 4 :   25000000  Priority 5 :   25000000
      Priority 6 :   25000000  Priority 7 :   25000000
      Sub pool unreserved BW
      Priority 0 :    3125000  Priority 1 :    3125000
      Priority 2 :    3125000  Priority 3 :    3125000
      Priority 4 :    3125000  Priority 5 :    3125000
      Priority 6 :    3125000  Priority 7 :    3125000
      Affinity Bit : 0


  Links in hash bucket 8.
    Link is associated with fragment 0. Link instance is 67441
      Link connected to Point-to-Point network
      Link ID : 10.1.1.1
      Interface Address : 10.10.25.4
      Neighbor Address : 10.10.25.5
      Admin Metric : 0
      Maximum bandwidth : 19440000
      Maximum global pool reservable bandwidth : 25000000
      Maximum sub pool reservable bandwidth    : 3125000
      Number of Priority : 8
      Global pool unreserved BW
      Priority 0 :   25000000  Priority 1 :   25000000
      Priority 2 :   25000000  Priority 3 :   25000000
      Priority 4 :   25000000  Priority 5 :   25000000
      Priority 6 :   25000000  Priority 7 :   25000000
      Sub pool unreserved BW
      Priority 0 :    3125000  Priority 1 :    3125000
      Priority 2 :    3125000  Priority 3 :    3125000
      Priority 4 :    3125000  Priority 5 :    3125000
      Priority 6 :    3125000  Priority 7 :    3125000
      Affinity Bit : 0
```

This table describes the significant fields shown in the display.

Table 15: show ospf mpls traffic-eng link Field Descriptions

Field	Description
Link ID	Link type.
Interface address	IP address of the interface.
Neighbor address	IP address of the neighbor.
Admin Metric	Administrative distance metric value used by Multiprotocol Label Switching traffic engineering (MPLS TE).
Maximum bandwidth	Bandwidth capacity of the link (in kbps).
Maximum global pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the global pool.
Maximum sub pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the subpool.
Number of Priority	Priority number.
Global pool unreserved BW	Amount of unreserved bandwidth that is available in the global pool.
Sub pool unreserved BW	Amount of unreserved bandwidth that is available in the subpool.
Affinity Bit	Used by MPLS TE. Attribute values required for links carrying this tunnel. A 32-bit dotted-decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

The following is sample output from the **show ospf mpls traffic-eng** command when the **fragment** keyword is specified:

```
RP/0/RP0:hostname# show ospf mpls traffic-eng fragment

            OSPF Router with ID (10.10.10.10) (Process ID 1)

  Area 0 has 2 MPLS TE fragment. Area instance is 67441.
  MPLS router address is 10.10.10.10
  Next fragment ID is 2

  Fragment 0 has 1 link. Fragment instance is 67441.
  Fragment has 1 link the same as last update.
  Fragment advertise MPLS router address
    Link is associated with fragment 0. Link instance is 67441
      Link connected to Point-to-Point network
      Link ID : 10.1.1.1
      Interface Address : 10.10.25.4
      Neighbor Address : 10.10.25.5
      Admin Metric : 0
      Maximum bandwidth : 19440000
      Maximum global pool reservable bandwidth : 25000000
      Maximum sub pool reservable bandwidth    : 3125000
      Number of Priority : 8
```

```
    Global pool unreserved BW
    Priority 0 :   25000000  Priority 1 :   25000000
    Priority 2 :   25000000  Priority 3 :   25000000
    Priority 4 :   25000000  Priority 5 :   25000000
    Priority 6 :   25000000  Priority 7 :   25000000
    Sub pool unreserved BW
    Priority 0 :    3125000  Priority 1 :    3125000
    Priority 2 :    3125000  Priority 3 :    3125000
    Priority 4 :    3125000  Priority 5 :    3125000
    Priority 6 :    3125000  Priority 7 :    3125000
    Affinity Bit : 0


Fragment 1 has 1 link. Fragment instance is 67441.
Fragment has 0 link the same as last update.
  Link is associated with fragment 1. Link instance is 67441
    Link connected to Point-to-Point network
    Link ID : 10.10.10.8
    Interface Address : 10.10.10.2
    Neighbor Address : 10.10.10.3
    Admin Metric : 0
    Maximum bandwidth : 19440000
    Maximum global pool reservable bandwidth : 25000000
    Maximum sub pool reservable bandwidth    : 3125000
    Number of Priority : 8
    Global pool unreserved BW
    Priority 0 :   25000000  Priority 1 :   25000000
    Priority 2 :   25000000  Priority 3 :   25000000
    Priority 4 :   25000000  Priority 5 :   25000000
    Priority 6 :   25000000  Priority 7 :   25000000
    Sub pool unreserved BW
    Priority 0 :    3125000  Priority 1 :    3125000
    Priority 2 :    3125000  Priority 3 :    3125000
    Priority 4 :    3125000  Priority 5 :    3125000
    Priority 6 :    3125000  Priority 7 :    3125000
    Affinity Bit : 0
```

This table describes the significant fields shown in the display.

Table 16: show ospf mpls traffic-eng fragment Field Descriptions

Field	Description
Area instance	Number of times traffic engineering information or any link changed.
Link instance	Number of times any link changed.
Link ID	Link type.
Interface address	IP address of the interface.
Neighbor address	IP address of the neighbor.
Admin Metric	Administrative distance metric value used by MPLS TE.
Maximum bandwidth	Bandwidth capacity of the link (in kbps).

Field	Description
Maximum global pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the global pool.
Maximum sub pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the subpool.
Number of Priority	Priority number.
Global pool unreserved BW	Amount of unreserved bandwidth that is available in the global pool.
Sub pool unreserved BW	Amount of unreserved bandwidth that is available in the subpool.
Affinity Bit	Used by MPLS TE. Attribute values required for links carrying this tunnel. A 32-bit dotted-decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

show ospf message-queue

To display the information about the queue dispatch values, peak lengths, and limits, use the **show ospf message-queue** command in XR EXEC mode.

show ospf message-queue

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf message-queue** command:

```
RP/0/RP0:hostname# show ospf 1 message-queue

OSPF 1
  Hello Input Queue:
    Current queue length: 0
    Event scheduled: 0
    Total queuing failures: 0
    Maximum length : 102
    Pkts pending processing: 0
    Limit: 5000

  Router Message Queue
    Current instance queue length: 0
    Current redistribution queue length: 0
    Current ex spf queue length: 0
    Current sum spf queue length: 0
    Current intra spf queue length: 0
    Event scheduled: 0
    Maximum length : 101
    Total low queuing failures: 0
    Total medium queuing failures: 0
    Total high queuing failures: 0
    Total instance events: 919
    Processing quantum : 300
```

```
    Low queuing limit: 8000
    Medium queuing limit: 9000
    High queuing limit: 9500
    Rate-limited LSA processing quantum: 150
    Current rate-limited LSA queue length: 0
    Rate-limited LSA queue peak len: 517

    Rate-limited LSAs processed: 4464
    Flush LSA processing quantum: 150
    Current flush LSA queue length: 0
    Flush LSA queue peak len: 274
    Rate-limited flush LSAs processed: 420

    SPF-LSA-limit processing quantum: 150
    Managed timers processing quantum: 50
    Instance message count: 0
    Instance pulse send count: 919
    Instance pulse received count: 919
    Global pulse count: 0
    Instance Pulse errors: 0

  TE Message Queue
    Current queue length: 0
    Total queuing failures: 0
    Maximum length : 0

Number of Dlink errors: 0
```

This table describes the significant fields shown in the display.

Table 17: show ospf message-queue Field Descriptions

Field	Description
Hello Input Queue	This section provides statistics on the number of events and incoming packets processed in the Hello (incoming packet) thread of the OSPF process.
Router Message Queue	This section provides statistics on the events and messages processed in the Router (primary) thread of the OSPF process.
TE Message Queue	This section provides statistics on traffic-engineering events and messages received by OSPF from TE (the te_control process). These events are processed in the Router thread of the OSPF process.
Number of Dlink errors	The number of enqueuing or dequeuing errors seen across all the linked-lists in the OSPF process.

Related Commands

Command	Description
queue dispatch incoming, on page 319	Limits the number of continuous incoming events processed.
queue dispatch rate-limited-lsa, on page 321	Sets the maximum number of rate-limited link-state advertisements (LSAs) processed per run.

Command	Description
queue dispatch spf-lsa-limit, on page 323	Limits the number of summary or external Type 3 to Type 7 link-state advertisements (LSAs) processed per shortest path first (SPF) run.
queue limit, on page 325	Sets the high watermark for incoming priority events.

show ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on an individual interface basis, use the **show ospf neighbor** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **neighbor** [{[*type interface-path-id*] [*neighbor-id*] [**detail**] | **area-sorted**}]

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.
area-id	(Optional) Area ID. If you do not specify an area, all areas are displayed.
type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors given in detail (lists all neighbors).
area-sorted	(Optional) Specifies that all neighbors are grouped by area.

Command Default

All neighbors

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf neighbor** command showing two lines of summary information for each neighbor:

```
RP/0/RP0:hostname# show ospf neighbor

Neighbors for OSPF

Neighbor ID     Pri  State          Dead Time  Address           Interface
192.168.199.137 1    FULL/DR        0:00:31    172.31.80.37      TenGigE0/3/0/5.20
    Neighbor is up for 18:45:22
192.168.48.1     1    FULL/DROTHER  0:00:33    192.168.48.1       TenGigE0/3/0/9.21
    Neighbor is up for 18:45:30
192.168.48.200   1    FULL/DROTHER  0:00:33    192.168.48.200     TenGigE0/3/0/9.21
    Neighbor is up for 18:45:25
192.168.199.137 5    FULL/DR        0:00:33    192.168.48.189     TenGigE0/3/0/9.21
    Neighbor is up for 18:45:27
```

This table describes the significant fields shown in the display.

Table 18: show ospf neighbor Field Descriptions

Field	Description
Neighbor ID	Neighbor router ID.
Pri	Designated router priority.
State	OSPF state.
Dead time	Time (in hh:mm:ss) that must elapse before OSPF declares the neighbor dead.
Address	Address of next hop.
Interface	Interface name of next hop.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.

The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
RP/0/RP0:hostname# show ospf neighbor 192.168.199.137

 Neighbor 192.168.199.137, interface address 172.31.80.37
    In the area 0.0.0.0 via interface TenGigE0/3/0/5.20
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x2
    Dead timer due in 0:00:32
    Neighbor is up for 18:45:30
    Number of DBD retrans during last exhange 0
    Index 1/1, 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 0 msec
 Neighbor 192.168.199.137, interface address 192.168.48.189
```

```
    In the area 0.0.0.0 via interface TenGigE0/3/0/9.21
    Neighbor priority is 5, State is FULL, 6 state changes
    Options is 0x2
    Dead timer due in 0:00:32
    Neighbor is up for 18:45:30
    Number of DBD retrans during last exhange 0
    Index 1/1, 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 0 msec

Total neighbor count: 2
```

This table describes the significant fields shown in the display.

Table 19: show ospf neighbor 192.168.199.137 Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of neighbor and neighbor state.
State	OSPF state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents(E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

If you specify the interface along with the neighbor ID, the software displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
RP/0/RP0:hostname# show ospf neighbor TenGigE0/3/0/5.20 192.168.199.137

 Neighbor 192.168.199.137, interface address 172.31.80.37
    In the area 0.0.0.0 via interface TenGigE0/3/0/5.20
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x2
```

```
    Dead timer due in 0:00:32
    Neighbor is up for 18:45:30
    Number of DBD retrans during last exhange 0
    Index 1/1, 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 0 msec

Total neighbor count: 1
```

This table describes the significant fields shown in the display.

Table 20: show ospf neighbor TenGigE0/3/0/5.20 192.168.199.137 Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor.
State	OSPF state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub)
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
RP/0/RP0:hostname# show ospf neighbor TenGigE0/3/0/9.21

Neighbors for OSPF ospf1

   ID          Pri   State        Dead Time     Address         Interface
192.168.48.1     1    FULL/DROTHER  0:00:33    192.168.48.1       TenGigE0/3/0/9.21
    Neighbor is up for 18:50:52
192.168.48.200   1    FULL/DROTHER  0:00:32    192.168.48.200     TenGigE0/3/0/9.21
    Neighbor is up for 18:50:52
192.168.199.137 5    FULL/DR       0:00:32    192.168.48.189     TenGigE0/3/0/9.21
```

```
    Neighbor is up for 18:50:52

Total neighbor count: 3
```

This table describes the significant fields shown in the display.

Table 21: show ospf neighbor TenGigE0/3/0/9.21 Field Descriptions

Field	Description
ID	Neighbor router ID.
Pri	Route priority of the neighbor.
State	OSPF state.
Dead Time	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Address	Address of next hop.
Interface	Interface name of next hop.
Neighbor is up	Time (in hh:mm:ss) that the OSPF neighbor has been up.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub)
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

The following samples are from output from the **show ospf neighbor detail** command:

```
RP/0/RP0:hostname# show ospf neighbor detail

 Neighbor 192.168.199.137, interface address 172.31.80.37
    In the area 0.0.0.0 via interface TenGigE0/3/0/5.20
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x2
    Dead timer due in 0:00:32
    Neighbor is up for 18:45:30
    Number of DBD retrans during last exhange 0
    Index 1/1, 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 0 msec

Total neighbor count: 1


 Neighbor 10.1.1.1, interface address 192.168.13.1
```

```
    In the area 0 via interface TenGigE0/3/0/9.21
    Neighbor priority is 1, State is FULL, 10 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x52
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:36
    Neighbor is up for 1w2d
    Number of DBD retrans during last exchange 0
    Index 3/3, retransmission queue length 0, number of retransmission 5
    First 0(0)/0(0) Next 0(0)/0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec

Neighbor 10.4.4.4, interface address 192.168.34.4
    In the area 0 via interface TenGigE0/3/0/5.20
    Neighbor priority is 1, State is FULL, 48 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x12
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:30
    Neighbor is up for 00:40:03
    Number of DBD retrans during last exchange 0
    Index 2/2, retransmission queue length 0, number of retransmission 6
    First 0(0)/0(0) Next 0(0)/0(0)
    Last retransmission scan length is 0, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

This table describes the significant fields shown in the display.

Table 22: show ospf neighbor detail Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of neighbor and neighbor state.
State	OSPF state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents. (E-bit only; possible values are 0 and 2; 2 indicates that the area is not a stub; 0 indicates that the area is a stub).)
LLS Options is 0x1 (LR)	Neighbor is NFS Cisco capable.
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.

Field	Description
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.

show ospf request-list

To display the first ten link-state requests pending that the local router is making to the specified Open Shortest Path First (OSPF) neighbor and interface, use the **show ospf request-list** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **request-list** [*type interface-path-id*] [*neighbor-id*]

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
vrf	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the OSPF VRF. The *vrf-name* argument can be specified as an arbitrary string. The strings “default” and “all” are reserved VRF names.
all	(Optional) Specifies all OSPF VRF instances.
area-id	(Optional) Area ID. If you do not specify an area, all areas are displayed.
type	Interface type.
i *nterface-path-id*	Physical interface or virtual interface. Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
neighbor-id	(Optional) IP address of the OSPF neighbor.

Command Default

All neighbors

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You might use this command when the databases of two neighboring routers are out of synchronization or if the adjacency does not form between them. Adjacency means that the routers synchronize their databases when they discover each other.

You can look at the list to determine if one router is trying to request a particular database update. Entries that are suspended in the list usually indicate that updates are not being delivered. One possible reason for this behavior is a maximum transmission unit (MTU) mismatch between the routers.

You might also look at this list to make sure it is not corrupted. The list should refer to database entries that actually exist.

Request list information is transient and normally the lists are empty.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf request-list** command:

```
RP/0/RP0:hostname# show ospf request-list 10.0.124.4 TenGigE0/3/0/9.21

Request Lists for OSPF pagent

 Neighbor 10.0.124.4, interface TenGigE0/3/0/9.21 address 10.3.1.2

 Type   LS ID            ADV RTR        Seq NO        Age   Checksum
    1   192.168.58.17     192.168.58.17   0x80000012     12   0x0036f3
    2   192.168.58.68     192.168.58.17   0x80000012     12   0x00083f
```

This table describes the significant fields shown in the display.

Table 23: show ospf request-list 10.0.124.4 TenGigE0/3/0/9.21 Field Descriptions

Field	Description
Neighbor	Specific neighbor receiving the request list from the local router.
Interface	Specific interface over which the request list is being sent.
Address	Address of the interface over which the request list is being sent.
Type	Type of link-state advertisement (LSA).
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of the advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of the LSA (in seconds).
Checksum	Checksum of the LSA.

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.

Command	Description
show ospf retransmission-list, on page 382	Displays the first ten link-state entries in the retransmission list that the local router sends to the specified neighbor over the specified interface.

show ospf retransmission-list

To display the first ten link-state entries in the Open Shortest Path First (OSPF) retransmission list that the local router sends to the specified neighbor over the specified interface, use the **show ospf retransmission-list** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] [*area-id*] **retransmission-list** [*type interface-path-id*] [*neighbor-id*]

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.
area-id	(Optional) Area ID. If you do not specify an area, all areas are displayed.
type	Interface type.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
neighbor-id	(Optional) IP address of the OSPF neighbor.

Command Default

All neighbors

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You might use this command when the databases of two neighboring routers are out of synchronization or if the adjacency is not forming between them. Adjacency means that the routers synchronize their databases when they discover each other.

You can look at the list to determine if one router is trying to request a particular database update. Entries that appear to be suspended in the list usually indicate that updates are not being delivered. One possible reason for this behavior is a maximum transmission unit (MTU) mismatch between the routers.

You might also look at this list to make sure it is not corrupted. The list should refer to database entries that actually exist.

Retransmission list information is transient, and normally the lists are empty.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf retransmission-list** command:

```
RP/0/RP0:hostname# show ospf retransmission-list 10.0.124.4 TenGigE0/3/0/9.21

 Neighbor 10.0.124.4, interface TenGigE0/3/0/9.21 address 10.3.1.2
```

This table describes the significant fields shown in the display.

Table 24: show ospf retransmission-list 10.0.124.4 TenGigE0/3/0/9.21 Field Descriptions

Field	Description
Neighbor	Specified neighbor receiving the retransmission list from the local router.
Interface	Specified interface over which the retransmission list is being sent.
Address	Address of the interface.

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.
show ospf request-list, on page 379	Displays the first ten link-state requests pending that the local router is making to the specified neighbor and interface.

show ospf routes

To display the Open Shortest Path First (OSPF) topology table, use the **show ospf routes** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] **routes** [{**connected** | **external** | **local**}] [*prefix mask*] [*prefix/length*] **[multicast-intact] [backup-path]**

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.
connected	(Optional) Displays connected routes.
external	(Optional) Displays routes redistributed from other protocols.
local	(Optional) Displays the local routes redistributed from the Routing Information Base (RIB).
prefix	(Optional) IP prefix, which limits output to a specific route. If the *prefix* argument is specified, either the *length* or *mask* argument is required.
mask	(Optional) IP address mask.
/ *length*	(Optional) Prefix length, which can be indicated as a slash (/) and number. For example, /8 indicates that the first eight bits in the IP prefix are network bits. If *length* is used, the slash is required.
multicast-intact **backup-path**	(Optional) Displays multicast intact paths. (Optional) Displays fast-reroute backup path information.
backup-path	(Optional) Displays fast-reroute backup path information.

Command Default

All route types

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show ospf routes** command to display the OSPF private routing table (which contains only routes calculated by OSPF). If there is something wrong with a route in the RIB, then it is useful to check the OSPF copy of the route to determine if it matches the RIB contents. If it does not match, there is a synchronization

problem between OSPF and the RIB. If the routes match and the route is incorrect, OSPF has made an error in its routing calculation.

Task ID

Task ID	Operations
ospf	read

show ospf routes command output with TI-LFA information

This is sample output from the **show ospf routes** command with **backup-path** keyword that displays backup-path information, including TI-LFA:

```
RP/0/RP0:hostnamesh ospf 1 routes 2.2.2.2/32 backup-path
Fri Apr  4 02:08:04.210 PDT

Topology Table for ospf 1 with ID 1.1.1.1

Codes: O - Intra area, O IA - Inter area
     O E1 - External type 1, O E2 - External type 2
     O N1 - NSSA external type 1, O N2 - NSSA external type 2

O    2.2.2.2/32, metric 3
     10.1.0.2, from 2.2.2.2, via TenGigE0/3/0/9.21, path-id 1
         Backup path: TI-LFA, P node: 4.4.4.4, Labels: 16004, 123
            10.0.3.2, from 2.2.2.2, via TenGigE0/3/0/5.20, protected bitmap 0x1
            Attribues: Metric: 104, SRLG Disjoint
```

This table describes the significant fields shown in the display.

Table 25: show ospf route Field Descriptions

Field	Description
O	OSPF route.
E	External Type 1 or 2 route.
N	NSSA Type 1 or 2
2.2.2.2/32	Network and subnet mask to which the local router has a route.
metric	Cost to reach network 10.3.1.0.
10.1.0.2	Next-hop router on the path to network 10.3.1.0.
from 2.2.2.2	Router ID 172.16.10.1 is the router that advertised this route.
via TenGigE0/3/0/9.21	Packets destined for the given prefix (10.3.1.0/24) are sent over TenGigE0/3/0/9.21.
Backup path	Indicates the topology independent loop-free alternate backup path. Here, the backup path uses the P node 4.4.4.4.

Examples

The following is sample output from the **show ospf routes** command:

```
RP/0/RP0:hostname# show ospf routes

Topology Table for ospf 1 with ID 10.3.4.2

Codes:O - Intra area, O IA - Inter area
       O E1 - External type 1, O E2 - External type 2
       O N1 - NSSA external type 1, O N2 - NSSA external type 2

O E2 10.3.1.0/24, metric 1
       10.3.4.1, from 172.16.10.1, via TenGigE0/1/0/3.50
O    10.3.4.0/24, metric 1562
       10.3.4.2, directly connected, via TenGigE0/1/0/3.50
O E2 10.1.0.0/16, metric 1
       10.3.4.1, from 172.16.10.1, via TenGigE0/1/0/3.50
O IA 10.10.10.0/24, metric 1572
       10.3.4.1, from 172.16.10.1, via TenGigE0/1/0/3.50
O E2 130.10.10.0/24, metric 20
       10.3.4.1, from 172.16.10.1, via TenGigE0/1/0/3.50
```

This table describes the significant fields shown in the display.

Table 26: show ospf route Field Descriptions

Field	Description
O	OSPF route.
E	External Type 1 or 2 route.
N	NSSA Type 1 or 2
10.3.1.0/24	Network and subnet mask to which the local router has a route.
metric	Cost to reach network 10.3.1.0.
10.3.4.1	Next-hop router on the path to network 10.3.1.0.
from 172.16.10.1	Router ID 172.16.10.1 is the router that advertised this route.
via TenGigE0/1/0/3.50	Packets destined for the given prefix (10.3.1.0/24) are sent over Ten Gigabit Ethernet interface 0/1/0/3.50.

The following is sample output from the **show ospf routes** command with a process name of 100:

```
RP/0/RP0:hostname# show ospf 100 routes

Topology Table for ospf 100 with ID 172.23.54.14

Codes:O - Intra area, O IA - Inter area
       O E1 - External type 1, O E2 - External type 2
       O N1 - NSSA external type 1, O N2 - NSSA external type 2

O    10.1.5.0/24, metric 1562
       10.1.5.14, directly connected, via TenGigE0/6/0/2.10
O IA 21.0.0.0/24, metric 1572
       10.1.5.12, from 172.23.54.12, via TenGigE0/6/0/2.10
O    10.0.0.0/24, metric 10
```

```
        10.0.0.12, directly connected, via TenGigE0/3/0/2.10
```

This table describes the significant fields shown in the display.

Table 27: show ospf 100 route Field Descriptions

Field	Description
O	OSPF route.
IA	Interarea route.
10.1.5.0/24	Network and subnet mask to which the local router has a route.
metric 1562	Cost to reach network 10.1.5.0.
10.1.5.14	Next-hop router on the path to network 10.1.5.0.
from 172.23.54.12	Router ID 172.23.54.12 is the router that advertised this route.
via TenGigE0/6/0/2.10	Packets destined for the given prefix (10.3.1.0/24) are sent over Ten Gigabit Ethernet interface 0/6/0/2.10.

The following is sample output from the **show ospf routes** command with a prefix of 10.0.0.0 and a length of 24:

```
RP/0/RP0:hostname# show ospf routes 10.0.0.0/24

Topology Table for ospf 100 with ID 172.23.54.14

Codes:O - Intra area, O IA - Inter area
       O E1 - External type 1, O E2 - External type 2
       O N1 - NSSA external type 1, O N2 - NSSA external type 2

O IA 10.0.0.0/24, metric 1572
       10.1.5.12, from 172.23.54.12, via TenGigE0/6/0/2.10
```

This table describes the significant fields shown in the display.

Table 28: show ospf route 10.0.0.0/24 Field Descriptions

Field	Description
O	Route is an OSPF route.
IA	Route to network 10.0.0.0 is an interarea route.
10.0.0.0/24	Network and subnet mask to which the local router has a route.
metric 1572	Cost to reach network 10.0.0.0.
10.1.5.12	IP address of next-hop router on the path to network 10.0.0.0.
from 172.23.54.12	Router ID 172.23.54.12 is the router that advertised this route.

Field	Description
via TenGigE0/6/0/2.10	Packets destined for the given prefix (10.0.0.0/24) are sent over Ten Gigabit Ethernet interface 0/6/0/2.10.

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.

show ospf statistics interface

To display the per interface statistics for OSPFv2, use the **show ospf statistics interface** command in XR EXEC mode.

show ospf [*process name* [*area id*]] [**vrf** {*vrf-name* | **all**}] [*area id*] **statistics interface** [{*interface name* | **summary-only**}]

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
area id	(Optional) Area number used to define the particular area.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings “default” and “all” are reserved VRF names.
summary-only	(Optional) Displays only the summary statistics for the given instance or area (if specified).

Command Default

No default behavior or values.

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf statistics interface** command:

```
RP/0/RP0:hostname# show ospf 0 1.1.1.1 statistics interface

        Interface POS0/3/0/0 Process ID 0 Area 1.1.1.1
 Multi-Adjacency Interface

  OSPF packet and LSA statistics
          RX(hello) RX(router)        TX     LSA RX     LSA TX
 Hello           32          -         33          -          -
```

```
DB Des           3          3          2          2          4
LS Req           0          0          1          0          0
LS Upd           5          5          3         18         10
LS Ack           1          1          3         10         18
TOTAL           41          9         42         30         32

 OSPF Header Errors

Version                  0        LLS                      0
Type                     0        Auth RX                  0
Length                   0        Auth TX                  0
Checksum                 0

 OSPF LSA Errors

Type                     0        Checksum                 0
Length                   0        Data                     0

 OSPF Errors

Bad Source               0        Area Mismatch            0
No Virtual Link          0        Self Originated          0
Nbr ignored              0        Graceful Shutdown        0
Unknown nbr              0        Passive intf             0
No DR/BDR                0        Disabled intf            0
Enqueue                  0        Unspecified RX           0
Socket                   0        Unspecified TX           0
```

This table describes the significant fields shown in the display.

Table 29: show ospf statistics interface Field Descriptions

Field	Description
OSPF packet and LSA statistics	Packets and LSAs received and transmitted on a given interface.
OSPF Header Errors	OSPF packets discarded due to the error in the OSPF header.
OSPF LSA Errors	OSPF LSAs discarded due to the error in the OSPF LSA header.
OSPF Errors	Packets discarded or errors encountered during handling OSPF packets on the given interface.

Related Commands

Command	Description
clear ospf statistics interface, on page 241	Clears the Open Shortest Path First (OSPF) statistics per interface.

show ospf summary-prefix

To display Open Shortest Path First (OSPF) aggregated summary address information, use the **show ospf summary-prefix** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] **summary-prefix**

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.

Command Default

All summary prefixes

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show ospf summary-prefix** command if you configured summarization of external routes with the **summary-prefix** command and you want to display configured summary addresses.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf summary-prefix** command:

```
RP/0/RP0:hostname# show ospf summary-prefix

OSPF Process 1, summary-prefix

10.1.0.0/255.255.0.0 Metric 20, Type 2, Tag 0
```

This table describes the significant fields shown in the display.

Table 30: show ospf summary-prefix Field Descriptions

Field	Description
10.1.0.0/255.255.0.0	Summary address designated for a range of addresses. The IP subnet mask used for the summary route.
Metric	Metric used to advertise the summary routes.
Type	External link-state advertisements (LSA) metric type.
Tag	Tag value that can be used as a "match" value for controlling redistribution through route maps.

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.
summary-prefix (OSPF), on page 405	Creates aggregate addresses for routes being redistributed from another routing protocol into the OSPF protocol.

show ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **show ospf virtual-links** command in XR EXEC mode.

show ospf [*process-name*] [**vrf** {*vrf-name* | **all**}] **virtual-links**

Syntax Description

process-name	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the **router ospf** command. If this argument is included, only information for the specified routing process is displayed.
vrf *vrf-name* **all**	(Optional) Specifies an OSPF VPN routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as an arbitrary string. The strings "default" and "all" are reserved VRF names.

Command Default

All virtual links

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show ospf virtual-links** command to display useful information for debugging OSPF routing operations.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospf virtual-links** command:

```
RP/0/RP0:hostname# show ospf virtual-links

Virtual Link to router 172.31.101.2 is up
Transit area 0.0.0.1, via interface TenGigE0/6/0/2.10, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

This table describes the significant fields shown in the display.

Table 31: show ospf virtual-links Field Descriptions

Field	Description
Virtual Link to router 172.31.101.2 is up	OSPF neighbor and whether the link to that neighbor is up or down.
Transit area 0.0.0.1	Transit area through which the virtual link is formed.
via interface TenGigE0/6/0/2.10	Interface through which the virtual link is formed.
Cost of usingusing 10	Cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	Transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	State of the OSPF neighbor.
Timer intervals	Various timer intervals (in seconds) configured for the link.
Hello due in 0:00:08	When the next hello message is expected from the neighbor (in hh:mm:ss).
Adjacency State FULL	Adjacency state between the neighbors.

Related Commands

Command	Description
router ospf, on page 338	Configures an OSPF routing process.

show protocols (OSPF)

To display information about the OSPFv2 processes running on the router, use the **show protocols** command in XR EXEC mode.

show protocols [{**afi-all** | **ipv4** | **ipv6**}] [{**all***protocol*}]

Syntax Description

afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies an IPv4 address family.
ipv6	(Optional) Specifies an IPv6 address family.
all	(Optional) Specifies all protocols for a given address family.
protocol	(Optional) Specifies a routing protocol. For the IPv4 address family, the options are: • **bgp** • **eigrp** • **isis** • **ospf** • **rip** For the IPv6 address family, the options are: • **bgp** • **eigrp** • **isis**

Command Default

No default behavior or value

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read
rib	read

Examples

The following is an OSPF configuration and the resulting **show protocols ospf** display:

```
  RP/0/RP0:hostname#show running router ospf

 router ospf 100
 nsr
 router-id 1.1.1.1
 nsf ietf
 address-family ipv4 unicast
 area 0
  interface Loopback1
   !
  interface TenGigE0/8/0/10
  !
  interface TenGigE0/13/0/0/10
  !
  interface TenGigE0/13/0/0/20
  !
  interface TenGigE0/15/0/7
  !
 !
!

  RP/0/RP0:hostname# show protocols ospf
  Routing Protocol OSPF 100
  Router Id: 1.1.1.1
  Distance: 110
  Non-Stop Forwarding: Enabled
  Redistribution:None
  Area 0
    Loopback1
    TenGigE0/2/0/1/6.100
    TenGigE0/13/0/0/10
    TenGigE0/13/0/0/20
    TenGigE0/15/0/7
```

This table describes the significant fields shown in the display.

Table 32: show protocols ospf Field Descriptions

Field	Description
Router Id	ID of the router for this configuration.
Distance	Administrative distance of OSPF routes relative to routes from other protocols.
Non-Stop Forwarding	Status of nonstop forwarding.
Redistribution	Lists the protocols that are being redistributed.
Area	Information about the current area including list of interfaces and the status of Multiprotocol Label Switching traffic engineering (MPLS TE).

snmp context (OSPF)

To specify an SNMP context for an OSPF instance, use the **snmp context** command in router configuration mode or in VRF configuration mode. To remove the SNMP context, use the **no** form of this command.

snmp context *context_name*
no snmp context *context_name*

Syntax Description

context_name	Specifies name of the SNMP context for OSPF instance.

Command Default

SNMP context is not specified.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The snmp-server commands need to be configured to perform SNMP request for the OSPF instance.

Note To map an SNMP context with a protocol instance, topology or VRF entity, use the **snmp-server context mapping** command. However, the **feature** option of this command does not work with OSPF protocol.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to configure an SNMP context *foo* for OSPF instance *100*:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 100
RP/0/RP0:hostname(config-ospf)#snmp context foo
```

This example shows how to configure **snmp-server** commands to be used with the **snmp context** command:

```
RP/0/RP0:hostname(config)#snmp-server host 10.0.0.2 traps version 2c public udp-port 1620
```

```
RP/0/RP0:hostname(config)#snmp-server community public RW
RP/0/RP0:hostname(config)#snmp-server contact foo
RP/0/RP0:hostname(config)#snmp-server community-map public context foo
```

This is a sample SNMP context configuration for OSPF instance *100*:

```
snmp-server host 10.0.0.2 traps version 2c public udp-port 1620
snmp-server community public RW
snmp-server contact foo

snmp-server community-map public context foo


router ospf 100
 router-id 2.2.2.2
 bfd fast-detect
 nsf cisco
snmp context foo
 area 0
  interface Loopback1
  !
 !
 area 1
  interface TenGigE0/2/0/1
   demand-circuit enable
  !
  interface TenGigE0/3/0/0
  !
  interface TenGigE0/3/0/1
  !
 !
!
```

Related Commands

Command	Description
snmp trap (OSPF)	Enables SNMP trap for an OSPF instance
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server community	Configures the community access string to permit access to the Simple Network Management Protocol (SNMP).
snmp-server contact	Sets the Simple Network Management Protocol (SNMP) system contact.
snmp-server community-map	Associates a Simple Network Management Protocol (SNMP) community with an SNMP context.

snmp trap (OSPF)

To enable SNMP trap for an OSPF instance, use the **snmp trap** command in VRF configuration mode. To disable SNMP trap for the OSPF instance, use the **no** form of this command.

snmp trap
no snmp trap

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled.

Command Modes

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to enable SNMP trap for OSPF instance *100* under VRF *vrf-1*:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 100
RP/0/RP0:hostname(config-ospf)#vrf vrf-1
RP/0/RP0:hostname(config-ospf-vrf)#snmp trap
```

Related Commands

Command	Description
snmp context (OSPF), on page 397	Specifies SNMP context for an OSPF instance.

snmp trap rate-limit (OSPF)

To control the number of traps that OSPF sends by configuring window size and the maximum number of traps during that window, use the **snmp trap rate-limit** command in router configuration mode. To disable configuring the window size and maximum number of traps during the window, use the **no** form of this command.

snmp trap rate-limit *window-size max-num-traps*
no snmp trap rate-limit *window-size max-num-traps*

Syntax Description

window-size	Specifies the trap rate limit sliding window size.
max-num-traps	Specifies the maximum number of traps sent in window time.

Command Default

none

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ospf	read,write

Examples

The following example shows how to set the trap rate limit sliding window size to 30 and the maximum number of traps sent to 100:

```
RP/0/RP0:hostname(config)#router ospf 100
RP/0/RP0:hostname(config-ospf)#snmp trap rate-limit 30 100
```

spf prefix-priority (OSPFv2)

To prioritize OSPFv2 prefix installation into the global Routing Information Base (RIB) during Shortest Path First (SPF) run, use the **spf prefix-priority** command in router configuration mode. To return to the system default value, use the **no** form of this command.

spf prefix-priority route-policy *policy-name*
no spf prefix-priority route-policy *policy-name*

Syntax Description

route-policy *policy-name* Specifies the route policy to apply to OSPFv2 prefix prioritization.

Note If SPF prefix prioritization is configured, /32 prefixes are no longer preferred by default. To retain the /32 prefixes in higher-priority queues, define the route-policy accordingly.

Command Default

SPF prefix prioritization is disabled.

Command Modes

OSPF router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SPF prefix prioritization is disabled, by default. In disabled mode, the /32 prefixes are installed into the global RIB before other prefixes.

If SPF prefix prioritization is enabled, routes are matched against the route-policy criteria and are assigned to the appropriate priority queue based on the spf-priority set. Unmatched prefixes, including the /32 prefixes, are placed in the low-priority queue.

If all /32 prefixes are desired in the high-priority queue or medium-priority queue, configure the following single route map:

```
prefix-set ospf-medium-prefixes
   0.0.0.0/0 ge 32
end-set
```

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure OSPFv2 SPF prefix prioritization:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# prefix-set ospf-critical-prefixes
RP/0/RP0:hostname(config-pfx)# 66.0.0.0/16
RP/0/RP0:hostname(config-pfx)# end-set
RP/0/RP0:hostname(config)# route-policy ospf-spf-priority
RP/0/RP0:hostname(config-rpl)# if destination in ospf-critical-prefixes then set
spf-priority critical
endif
RP/0/RP0:hostname(config-rpl)# end-policy
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# router-id 66.0.0.1
RP/0/RP0:hostname(config-ospf)# spf prefix-priority route-policy ospf-spf-priority
```

Related Commands

Command	Description
prefix-set	Enters prefix set configuration mode and defines a prefix set.
route-policy (RPL)	Defines a route policy and enters route-policy configuration mode.

stub (OSPF)

To define an area as a stub area, use the **stub** command in area configuration mode. To disable this function, use the **no** form of this command.

stub [**no-summary**]
no stub

Syntax Description

no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Command Default

No stub area is defined.

Command Modes

Area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You must configure the **stub** command on all routers in the stub area.

Use the **default-cost** command on the ABR of a stub area to specify the cost of the default route advertised into the stub area by the ABR.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending summary LSAs (LSA Type 3) into the stub area.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to assign a default cost of 20 to stub network 10.0.0.0:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# area 10.0.0.0
RP/0/RP0:hostname(config-ospf-ar)# stub
RP/0/RP0:hostname(config-ospf-ar)# default-cost 20
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Related Commands

Command	Description
authentication (OSPF), on page 227	Enables authentication for an OSPF area.
default-cost (OSPF), on page 249	Specifies a cost for the default summary route sent into a stub area.

summary-prefix (OSPF)

To create aggregate addresses for routes being redistributed from another routing protocol into the Open Shortest Path First (OSPF) protocol, use the **summary-prefix** command in the appropriate mode. To stop summarizing redistributed routes, use the **no** form of the command.

summary-prefix *address mask* [{**not-advertise** | **tag** *tag*}]
no summary-prefix *address mask*

Syntax Description

address	Summary address designated for a range of addresses.
mask	IP subnet mask used for the summary route.
not-advertise	(Optional) Suppresses summary routes that match the address and mask pair from being advertised.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution through route policies.

Command Default

When this command is not used, specific addresses are created for each route from another route source being distributed into the OSPF protocol.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **summary-prefix** command to cause an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. This command summarizes only routes from other routing protocols that are being redistributed into OSPF.

You can use this command multiple times to summarize multiple groups of addresses. The metric used to advertise the summary is the lowest metric of all the more specific routes. This command helps reduce the size of the routing table.

If you want to summarize routes between OSPF areas, use the **range** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

In the following example, summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# summary-prefix 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
range (OSPF), on page 327	Consolidates and summarizes routes at an area boundary.

timers lsa group-pacing

To change the interval at which Open Shortest Path First (OSPF) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa group-pacing** command in the appropriate mode. To restore the default value, use the **no** form of this command.

timers lsa group-pacing *seconds*
no timers lsa group-pacing

Syntax Description

seconds	Interval (in seconds) at which LSAs are grouped and refreshed, checksummed, or aged. Range is 10 seconds to 1800 seconds.

Command Default

seconds : 240 seconds

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate and you need not configure this feature.

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have approximately 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to change the OSPF pacing between LSA groups to 60 seconds:

```
RP/0/RP0:hostname# configure
 RP/0/RP0:hostname(config)# router ospf 1
 RP/0/RP0:hostname(config-ospf)# timers lsa group-pacing 60
```

timers lsa min-arrival

To limit the frequency that new instances of any particular Open Shortest Path First (OSPF) link-state advertisements (LSAs) can be accepted during flooding, use the **timers lsa min-arrival** command in the appropriate mode. To restore the default value, use the **no** form of this command.

timers lsa min-arrival *milliseconds*

no timers lsa min-arrival

Syntax Description

milliseconds	Minimum interval (in milliseconds) between accepting same LSA. Range is 0 to 600000 milliseconds.

Command Default

milliseconds : 100 milliseconds

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to change the minimum interval between accepting the same LSA to 2 seconds:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# timers lsa min-arrival 2
```

timers lsa refresh

To configure the time interval at which Open Shortest Path First (OSPF) self-originated link-state advertisements (LSAs) are refreshed, use the **timers lsa refresh** command in an appropriate configuration mode. To restore the default value, use the **no** form of this command.

timers lsa refresh *seconds*
no timers lsa refresh

Syntax Description

seconds	How often self-originated LSAs should be refreshed, in seconds. Range is 1800 to 2700 seconds.

Command Default

seconds : 1800 seconds.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

timers lsa refresh command allows self-originated LSAs to be refreshed at non-standard times, anywhere from 1800 to 2700 seconds. Higher refresh interval value may gradually lead to lower CPU utilization by OSPF process.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure an LSA refresh interval of 1800 seconds:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 100
RP/0/RP0:hostname(config-ospf)# timers lsa refresh 1800
```

Related Commands

Command	Description
timers lsa group-pacing, on page 407	Change the interval at which Open Shortest Path First (OSPF) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged.

Command	Description
timers lsa min-arrival, on page 408	Limits the frequency that new instances of any particular Open Shortest Path First (OSPF) link-state advertisements (LSAs) can be accepted during flooding.

timers throttle lsa all (OSPF)

To modify the Open Shortest Path First (OSPF) link-state advertisement (LSA) throttling, use the **timers throttle lsa all** command in the appropriate mode. To revert LSA throttling to default settings, use the **no** form of this command

timers throttle lsa all *start-interval hold-interval max-interval*
no timers throttle lsa all

Syntax Description

start-interval	Delay to generate first occurance of LSA in milliseconds. Range is 0 to 600000 milliseconds.
hold-interval	Minimum delay between originating the same LSA in milliseconds. Range is 1 to 600000 milliseconds.
max-interval	Maximum delay between originating the same LSA in milliseconds. Range is 1 to 600000 milliseconds.

Command Default

start-interval : 50 milliseconds

hold-interval : 200 milliseconds

max-interval : 5000 milliseconds

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The *lsa-start* time is the delay before flooding the first instance of an LSA. The *lsa-hold* interval is the minimum time to elapse before flooding an updated instance of an LSA. The *lsa-max-wait* time is the maximum time that can elapse before flooding an updated instance of an LSA.

For quick convergence, use smaller times for the *lsa-start* time and *lsa-hold* interval. However, in relatively large networks, this may result in a large number of LSAs being flooded in a relatively short time. A balance with the *lsa-start* time and *lsa-hold* interval can be iteratively arrived at for the size of your network. The *lsa-max-wait* time can be used to ensure that OSPF reconverges within a reasonable amount of time.

Note LSA throttling is always enabled. You can change the timer values with the **timers throttle lsa all** command or specify the **no** keyword to revert back to the default settings.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to change the start, hold, and maximum wait interval values to 500, 1000, and 90,000 milliseconds, respectively:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# timers throttle lsa all 500 1000 90000
```

The following example is output from the show ospf command that displays the modified LSA throttle settings:

```
RP/0/RP0:hostname# show ospf

Routing Process "ospf 1" with ID 1.1.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
 Minimum hold time for LSA throttle 1000 msecs
 Maximum wait time for LSA throttle 90000 msecs
 Minimum LSA interval 1000 msecs. Minimum LSA arrival 1 secs
 Maximum number of configured interfaces 255
 Number of external LSA 0. Checksum Sum 00000000
 Number of opaque AS LSA 0. Checksum Sum 00000000
 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 2. 2 normal 0 stub 0 nssa
 External flood list length 0
 Non-Stop Forwarding enabled
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 2
        SPF algorithm executed 8 times
        Number of LSA 2. Checksum Sum 0x01ba83
        Number of opaque link LSA 0. Checksum Sum 00000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 1
        Number of interfaces in this area is 1
        SPF algorithm executed 9 times
        Number of LSA 2. Checksum Sum 0x0153ea
        Number of opaque link LSA 0. Checksum Sum 00000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Related Commands

Command	Description
show ospf, on page 340	Displays generic information about OSPF routing processes.

timers throttle spf (OSPF)

To modify the Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the **timers throttle spf** command in the appropriate mode. To revert SPF throttling to default settings, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*
no timers throttle spf

Syntax Description

spf-start	Initial SPF schedule delay (in milliseconds). Range is 1 to 600000 milliseconds.
spf-hold	Minimum hold time (in milliseconds) between two consecutive SPF calculations. Range is 1 to 600000 milliseconds.
spf-max-wait	Maximum wait time (in milliseconds) between two consecutive SPF calculations. Range is 1 to 600000 milliseconds.

Command Default

spf-start:50 milliseconds

spf-hold: 200 milliseconds

spf-max-wait: 5000 milliseconds

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The *spf-start* time is the delay before running SPF for the first time. The *spf-hold* interval is the minimum time to elapse between subsequent SPF runs. The *spf-max-wait* time is the maximum time that can elapse before running SPF again.

Tip Setting a low *spf-start* time and *spf-hold* time causes routing to switch to the alternate path more quickly if there is a failure; however, it consumes more CPU processing time.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to change the start, hold, and maximum wait interval values to 5, 1000, and 90000 milliseconds, respectively:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# timers throttle spf 5 1000 90000
```

transmit-delay (OSPF)

To set the estimated time required to send a link-state update packet on the interface, use the **transmit-delay** command in the appropriate mode. To return to the default value, use the **no** form of this command.

transmit-delay *seconds*
no transmit-delay *seconds*

Syntax Description

seconds	Time (in seconds) required to send a link-state update. Range is 1 to 65535 seconds.

Command Default

seconds: 1 second

Command Modes

Router configuration

Area configuration

Interface configuration

Virtual-link configuration

VRF configuration

Multi-area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link,the time in which the LSA propagates over the link is not considered. This setting has significance only on very low-speed networks not supported in the Cisco IOS XR software or on networks such as satellite circuits that incur a very long (greater than one second) delay time.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure a transmit delay for interface TenGigE0/6/0/2.10:

```
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# transmit-delay 3
```

Related Commands

Command	Description
show ospf, on page 340	Displays general information about OSPF routing processes.

ucmp (OSPFv2)

To enable unequal cost multipath (UCMP) calculation for Open Shortest Path First version 2 (OSPFv2) , use the **ucmp** command in an appropriate OSPF configuration mode. To disable UCMP for OSPFv2, use the **no** form of this command.

ucmp [**prefix-list** *prefix-list-name*] [**variance** *value*]
no ucmp

Syntax Description

prefix-list	(Optional) Specifies prefix-list name to filter UCMP paths based on prefixes.
prefix-list-name	Name of the prefix-list to be specified to filter UCMP paths.
variance	(Optional) Specifies variance parameter to filter UCMP paths based on cost.
variance-value	Variance value. The variance value is expressed in terms of percentage of the Primary path metric. Range is from 101 to 10000. Default variance value is 200.

Command Default

UCMP is disabled.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Enabling the **ucmp** command makes the router calculate UCMP nexthops for all prefixes in the routing table.

The UCMP path calculation can be controlled such that UCMP nexthops are calculated only for a certain set of prefixes. Use the **ucmp** command with the **prefix-set** option to enable this functionality.

If there are multiple UCMP nexthops with various metrics, then the selection of the number of UCMP nexthops is controlled by the **variance** option in the UCMP command. The variance value is expressed in terms of percentage of the primary path metric. For example, if the variance value is 150 and the primary path metric is 100, then select all the UCMP nexthops with metrics from 101 to 150.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to enable calculation of UCMP nexthops for all the prefixes in the routing table:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 1
RP/0/RP0:hostname(config-ospf)#ucmp
```

This example shows how to enable calculation of UCMP nexthops for a set of prefixes in the prefix-list *list1*:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 1
RP/0/RP0:hostname(config-ospf)#ucmp prefix-list list1
```

This example shows how to enable calcualtion of UCMP mexthops with variance value *120*:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 1
RP/0/RP0:hostname(config-ospf)#ucmp variance 120
```

Related Commands

Command	Description
ucmp delay-interval (OSPFv2), on page 420	Specifies delay between primary SPF completion and start of UCMP computation.
ucmp exclude interface (OSPFv2), on page 422	Excludes an interface from unequal cost multipath (UCMP) computation.
bandwidth	Configures the bandwidth of an interface.

ucmp delay-interval (OSPFv2)

To specify delay between primary SPF completion and start of UCMP computation, use the **ucmp delay-interval** command in an appropriate OSPF configuration mode. To disable this functionality, use the **no** form of this command.

ucmp delay-interval *delay-interval*
no ucmp delay-interval

Syntax Description

delay-interval	Delay interval value in milliseconds. Range is from 100 to 65535 . The default value for the interval is 100.

Command Default

UCMP delay interval is set to 100 milliseconds.

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to set the delay between primary SPF completion and the start of UCMP computation, to 800 milliseconds:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 1
RP/0/RP0:hostname(config-ospf)#ucmp delay-interval 800
```

Related Commands

Command	Description
ucmp (OSPFv2), on page 418	Enables unequal cost multipath (UCMP) calculation for OSPFv2.
ucmp exclude interface (OSPFv2), on page 422	Excludes an interface from unequal cost multipath (UCMP) computation.

Command	Description
bandwidth	Configures the bandwidth of an interface.

ucmp exclude interface (OSPFv2)

To exclude an interface from unequal cost multipath (UCMP) computation, use the **ucmp exclude interface** command in an appropriate OSPF configuration mode. To disable this functionality, use the **no** form of this command.

ucmp exclude interface *type interface-path-id*
no ucmp exclude interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

none

Command Modes

Router configuration

VRF configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **ucmp exclude interfac**e command to exclude an interface from being selected as a UCMP backup path.

Task ID

Task ID	Operation
ospf	read, write

This example shows how to exclude interface POS 0/3/0/1 from UCMP computation:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 1
RP/0/RP0:hostname(config-ospf)#ucmp exclude interface GiganitEthernet 0/3/0/1
```

Related Commands

Command	Description
ucmp (OSPFv2), on page 418	Enables unequal cost multipath (UCMP) calculation for OSPFv2.
ucmp delay-interval (OSPFv2), on page 420	Specifies delay between primary SPF completion and start of UCMP computation.
bandwidth	Configures the bandwidth of an interface.

virtual-link (OSPF)

To define an Open Shortest Path First (OSPF) virtual link, use the **virtual-link** command in area configuration mode. To remove a virtual link, use the **no** form of this command.

virtual-link *router-id*
no virtual-link *router-id*

Syntax Description

router-id	Router ID associated with the virtual link neighbor. The router ID appears in the **show ospf** command display. The router ID can be any 32-bit router ID value specified in four-part, dotted-decimal notation.

Command Default

No virtual links are defined.

Command Modes

Area configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

All areas in an OSPF autonomous system must be physically connected to the backbone area (area 0). In some cases in which this physical connection is not possible, you can use a virtual link to connect to the backbone through a nonbackbone area. You can also use virtual links to connect two parts of a partitioned backbone through a nonbackbone area. The area through which you configure the virtual link, known as a transit area, must have full routing information. The transit area cannot be a stub or not-so-stubby area.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to establish a virtual link with default values for all optional parameters:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# area 10.0.0.0
RP/0/RP0:hostname(config-ospf-ar)# virtual-link 10.3.4.5
RP/0/RP0:hostname(config-ospf-ar-vl)#
```

The following example shows how to establish a virtual link with clear text authentication called mykey:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 201
RP/0/RP0:hostname(config-ospf)# area 10.0.0.0
RP/0/RP0:hostname(config-ospf-ar)# virtual-link 10.3.4.5
RP/0/RP0:hostname(config-ospf-ar-vl)# authentication-key 0 mykey
```

Related Commands

Command	Description
authentication (OSPF), on page 227	Enables authentication for an OSPF area.
show ospf virtual-links, on page 393	Displays parameters and the current state of OSPF virtual links

vrf (OSPF)

To configure an Open Shortest Path First (OSPF) VPN routing and forwarding (VRF) instance, use the **vrf** command in router configuration mode. To terminate an OSPF VRF, use the **no** form of this command.

vrf *vrf-name*
no vrf *vrf-name*

Syntax Description

vrf-name	Identifier of an OSPF VRF. The *vrf-name* argument can be specified as an arbitrary string. The strings “default” and “all” are reserved VRF names.

Command Default

No OSPF VRF is defined.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task ID's. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **vrf** command to explicitly configure a VRF. Commands configured under the VRF configuration mode (such as the **interface** [OSPF] and **authentication** commands) are automatically bound to that VRF.

To modify or remove the VRF, the *vrf-id* argument format must be the same as the format used when creating the area.

Note To remove the specified VRF from the router configuration, use the **no vrf** *vrf-id* command. The **no vrf** *vrf-id* command removes the VRF and all VRF options, such as **authentication** , **default-cost** , **nssa** , **range** , **stub** , **virtual-link** , and **interface.**

To avoid possibly having the router ID change under a VRF, explicitly configure the router ID using the **router-id** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure VRF vrf1 and Ten Gigabit Ethernet interface 0/6/0/2.10. Ten Gigabit Ethernet interface 0/6/0/2.10 is bound to VRF vrf1 automatically.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf 1
RP/0/RP0:hostname(config-ospf)# vrf vrf1
RP/0/RP0:hostname(config-ospf-vrf)# area area1
RP/0/RP0:hostname(config-ospf-vrf-ar)# interface TenGigE0/6/0/2.10
```

Related Commands

Command	Description
router-id (OSPF), on page 336	Configures a router ID for an OSPF process.

IS-IS Command Reference

This chapter describes the commands to configure IS-IS.

address-family (IS-IS)

To enter address family configuration mode for configuring Intermediate System-to-Intermediate System (IS-IS) routing that use standard IP Version 4 (IPv4)address prefixes, use the **address-family** command in router configuration or interface configuration mode. To disable support for an address family, use the **no** form of this command.

address-family {**ipv4**} {**unicast**}
no address-family {**ipv4**} {**unicast**}

Syntax Description

ipv4	Specifies IPv4 address prefixes.
unicast	Specifies unicast address prefixes.

Command Default

An address family is not specified. The default subaddress family (SAFI) is unicast.

Command Modes

Router configuration

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **address family** command to place the router or interface in address family configuration mode. In router address family configuration mode, you can configure routing that uses standard IPv4 address prefixes. An address family must be specified in interface configuration mode. In interface address family configuration mode, you can alter interface parameters for IPv4.

You must specify an address family in order to configure parameters that pertain to a single address family.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure the IS-IS router process with IPv4 unicast address prefixes:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE interface 0/1/0/0
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-if-af)#
```

adjacency-check disable

To suppress Intermediate System-to-Intermediate System (IS-IS) IP Version 4 (IPv4) protocol-support consistency checks that are performed prior to forming adjacencies on hello packets, use the **adjacency-check disable** command in address family configuration mode. To remove this function, use the **no** form of this command.

adjacency-check disable
no adjacency-check disable

Command Default

Adjacency check is enabled

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

IS-IS performs consistency checks on hello packets and forms an adjacency only with a neighboring router that supports the same set of protocols. A router running IS-IS for both IPv4 does not form an adjacency with a router running IS-IS for IPv4 only.

Use the **adjacency-check disable** command to allow an IPv4 IS-IS router to form an adjacency with a router running IPv4 IS-IS.

In addition, the **adjacency-check disable** command suppresses the IPv4 subnet consistency check and allows IS-IS to form an adjacency with other routers regardless of whether they have an IPv4 subnet in common.

Task ID

Task ID	Operations
isis	read, write

Examples

The command in the following example disables the adjacency checks:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4
RP/0/RP0:hostname(config-isis-af)# adjacency-check disable
```

advertise passive-only

To configure IS-IS to advertise only prefixes that belong to passive interfaces, use the **advertise-passive-only** command in ISIS address family configuration mode. To disable advertisement only prefixes that belong to passive interfaces, use the **no** form of this command.

advertise passive-only
no advertise passive-only

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

IPv4 unicast address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operation
isis	read, write

This example shows how to configure IS-IS to advertise only prefixes that belong to passive interfaces.

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router isis isp
RP/0/RP0:hostname(config-isis)#address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)#advertise passive-only
```

attached-bit receive ignore

To ignore the attached bit in a received Level 1 link-state packet (LSP), use the **attached-bit receive ignore** command in address family configuration mode. To remove the **attached-bit receive ignore** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

attached-bit receive ignore
no attached-bit receive ignore

Command Default

The attached bit is set in the LSP.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure to ignore the attached bit in a received LSP:

```
RP/0/RP0:hostname(config)# router isis isp1
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# attached-bit receive ignore
```

attached-bit send

To configure an Intermediate System-to-Intermediate System (IS-IS) instance with an attached bit in the Level 1 link-state packet (LSP), use the **attached-bit send** command in address family configuration mode. To remove the **attached-bit send** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

attached-bit send {**always-set** | **never-set**}
no attached-bit send {**always-set** | **never-set**}

Syntax Description

always-set	Specifies to always set the attached bit in the LSP.
never-set	Specifies to never set the attached bit in the LSP.

Command Default

The attached bit is not forced to be set or unset in the LSP.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **attached-bit send** command to set an IS-IS instance with an attached bit in the Level 1 LSP that allows another IS-IS instance to redistribute Level 2 topology. The attached bit is used when the Level 2 connectivity from another IS-IS instance is advertised by the Level 1 attached bit.

The attached bit is configured for a specific address family only if the **single-topology** command is not configured.

Note If connectivity for the Level 2 instance is lost, the attached bit in the Level 1 instance LSP continues sending traffic to the Level 2 instance and causes the traffic to be dropped.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure an Intermediate System-to-Intermediate System (IS-IS) instance with an attached bit:

```
RP/0/RP0:hostname(config)# router isis isp1
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# attached-bit send always-set
```

Related Commands

Command	Description
retransmit-interval (IS-IS), on page 501	Redistribute routes from one routing protocol into Intermediate System-to-Intermediate System (IS-IS).

circuit-type

To configure the type of adjacency used for the Intermediate System-to-Intermediate System (IS-IS) protocol, use the **circuit-type** command in interface configuration mode. To reset the circuit type to Level l and Level 2, use the **no** form of this command.

circuit-type {**level-1** | **level-1-2** | **level-2-only**}
no circuit-type

Syntax Description

level-1	Establishes only Level 1 adjacencies over an interface.
level-1-2	Establishes both Level 1 and Level 2 adjacencies, if possible.
level-2-only	Establishes only Level 2 adjacencies over an interface.

Command Default

Default adjacency types are Level 1 and Level 2 adjacencies.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Adjacencies may not be established even if allowed by the **circuit-type** command. The proper way to establish adjacencies is to configure a router as a Level 1, Level 1 and Level 2, or Level 2-only system command. Only on networking devices that are between areas (Level 1 and Level 2 networking devices) should you configure some interfaces to be Level 2-only to prevent wasting bandwidth by sending out unused Level 1 hello packets. Remember that on point-to-point interfaces, the Level 1 and Level 2 hello packets are in the same packet.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure a Level 1 adjacency with its neighbor on TenGigE interface 0/2/0/0 and Level 2 adjacencies with all Level 2-capable routers on TenGigE interface 0/5/0/2:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# is-type level-1-2
RP/0/RP0:hostname(config-isis)# interface TenGigE interface 0/2/0/0
RP/0/RP0:hostname(config-isis-if)# circuit-type level-1
RP/0/RP0:hostname(config-isis-if)# exit
RP/0/RP0:hostname(config-isis)# interface TenGigE interface 0/5/0/2
RP/0/RP0:hostname(config-isis-if)# circuit-type level-2-only
```

In this example, only Level 2 adjacencies are established because the **is-type** command is configured:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# is-type level-2-only
RP/0/RP0:hostname(config-isis)# interface TenGigE interface 0/2/0/0
RP/0/RP0:hostname(config-isis-if)# circuit-type level-1-2
```

clear isis process

To clear the link-state packet (LSP) database and adjacency database sessions for an Intermediate System-to-Intermediate System (IS-IS) instance or all IS-IS instances, use the **clear isis process** command.

clear isis [**instance** *instance-id*] **process**

Syntax Description

instance *instance-id*	(Optional) Specifies IS-IS sessions for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **clear isis process** command without any keyword to clear all the IS-IS instances. Add the **instance** *instance-id* keyword and argument to clear the specified IS-IS instance.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows the IS-IS LSP database and adjacency sessions being cleared for instance 1:

```
RP/0/RP0:hostname# clear isis instance 1 process
```

clear isis route

To clear the Intermediate System-to-Intermediate System (IS-IS) routes in a topology, use the **clear isis route** command.

clear isis [**instance** *instance-id*] {**afi-all** | **ipv4**} {**unicast** | **safi-all**} [**topology** *topo-name*] **route**

Syntax Description

instance *instance-id*	(Optional) Specifies IS-IS sessions for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
afi-all	Specifies IP Version 4 (IPv4) address prefixes.
ipv4	Specifies IPv4 address prefixes.
unicast	Specifies unicast address prefixes.
safi-all	Specifies all secondary address prefixes.
topology *topo-name*	(Optional) Specifies topology table information and name of the topology table.

Command Default

No default behavior or value

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **clear isis route** command to clear the routes from the specified topology or all routes in all topologies if no topology is specified.

Task ID

Task ID	Operations
isis	execute
rib	read, write
basic-services	read, write

Examples

The following example shows how to clear the routes with IPv4 unicast address prefixes:

```
RP/0/RP0:hostname# clear isis ipv4 unicast route
```

clear isis statistics

To clear the Intermediate System-to-Intermediate System (IS-IS) statistics, use the **clear isis statistics** command.

clear isis [**instance** *instance-id*] **statistics** [*type interface-path-id*]

Syntax Description

instance *instance-id*	(Optional) Clears IS-IS sessions for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **clear isis statistics** command to clear the information displayed by the **show isis statistics** command.

Task ID

Task ID	Operations
isis	execute
rib	read, write
basic-services	read, write

Examples

The following example shows the IS-IS statistics for a specified interface being cleared:

```
RP/0/RP0:hostname# clear isis instance 23 statistics
```

csnp-interval

To configure the interval at which periodic complete sequence number PDU (CSNP) packets are sent on broadcast interfaces, use the **csnp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

csnp-interval *seconds* [**level** {**1** | **2**}]
no csnp-interval *seconds* [**level** {**1** | **2**}]

Syntax Description

seconds	Interval (in seconds) of time between transmission of CSNPs on multiaccess networks. This interval applies only for the designated router. Range is 0 to 65535 seconds.
level { **1** | **2** }	(Optional) Specifies the interval of time between transmission of CSNPs for Level 1 or Level 2 independently.

Command Default

seconds : 10 seconds

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **csnp-interval** command applies only to the designated router (DR) for a specified interface. Only DRs send CSNP packets to maintain database synchronization. The CSNP interval can be configured independently for Level 1 and Level 2.

Use of the **csnp-interval** command on point-to-point subinterfaces makes sense only in combination with the IS-IS mesh-group feature.

Task ID

Task ID	Operations
isis	execute
rib	read, write
basic-services	read, write

Examples

The following example shows how to set the CSNP interval for Level 1 to 30 seconds:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE interface 0/0/2/0
RP/0/RP0:hostname(config-isis-if)# csnp-interval 30 level 1
```

default-information originate (IS-IS)

To generate a default route into an Intermediate System-to-Intermediate System (IS-IS) routing domain, use the **default-information originate** command in address family configuration mode. To remove the **default-information originate** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

default-information originate [{**external** | **route-policy** *route-policy-name*}]
no default-information originate [{**external** | **route-policy** *route-policy-name*}]

Syntax Description

route-policy	(Optional) Defines the conditions for the default route.
route-policy-name	(Optional) Name for the route policy.

Command Default

A default route is not generated into an IS-IS routing domain.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If a router configured with the **default-information originate** command has a route to 0.0.0.0 in the routing table, IS-IS originates an advertisement for 0.0.0.0 in its link-state packets (LSPs).

Without a route policy, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another process to find the default route, which is to look for the closest Level 1 and Level 2 router. The closest Level 1 and Level 2 router can be found by looking at the attached-bit (ATT) in Level 1 LSPs.

A route policy can be used for two purposes:

- To make the router generate the default route in its Level 1 LSPs.
- To advertise 0.0.0.0/0 conditionally.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to generate a default external route into an IS-IS domain:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# default-information originate
```

disable (IS-IS)

To disable the Intermediate System-to-Intermediate System (IS-IS) topology on a specified interface, use the **disable** command in interface address family configuration mode. To remove this function, use the **no** form of this command.

disable
no disable

Command Default

IS-IS protocol is enabled.

Command Modes

Interface address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to disable the IS-IS protocol for IPv4 unicast on TenGigE interface 0/1/0/1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE interface 0/1/0/1
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-if-af)# disable
```

distance (IS-IS)

To define the administrative distance assigned to routes discovered by the Intermediate System-to-Intermediate System (IS-IS) protocol, use the **distance** command in address family configuration mode. To remove the **distance** command from the configuration file and restore the system to its default condition in which the software removes a distance definition, use the **no** form of this command.

distance *weight* [{*prefix maskprefix/length* | [{*prefix-list-name*}]}]
no distance [{*weight*}] [{*prefix maskprefix/length* | [{*prefix-list-name*}]}]

Syntax Description

weight	Administrative distance to be assigned to IS-IS routes. Range is 1 to 255.
prefix	(Optional) The *prefix* argument specifies the IP address in four-part, dotted-decimal notation.
mask	(Optional) IP address mask.
/length	(Optional) The length of the IP prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value. Range is 0 to 32 for IPv4 addresses.
prefix-list-name	(Optional) List of routes to which administrative distance applies.

Command Default

weight : 115

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

An administrative distance is an integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

Use the **distance** command to configure the administrative distances applied to IS-IS routes when they are inserted into the Routing Information Base (RIB), and influence the likelihood of these routes being preferred over routes to the same destination addresses discovered by other protocols.

The *address/prefix-length* argument defines to which source router the distance applies. In other words, each IS-IS route is advertised by another router, and that router advertises an address that identifies it. This source address is displayed in the output of the **show isis route detail** command.

The **distance** command applies to the routes advertised by routers whose address matches the specified prefix. The *prefix-list-name* argument can then be used to refine this further so that the **distance** command affects only specific routes.

Task ID

Task ID	Operations
isis	read, write

Examples

In the following example, a distance of 10 is assigned to all routes to 2.0.0.0/8 and 3.0.0.0/8 (or more specific prefixes) that are advertised by routers whose ID is contained in 1.0.0.0/8. A distance of 80 is assigned to all other routes.

```
RP/0/RP0:hostname# ipv4 prefix-list target_routes
RP/0/RP0:hostname(config-ipv4_pfx)# permit 2.0.0.0/8
RP/0/RP0:hostname(config-ipv4_pfx)# permit 3.0.0.0/8
RP/0/RP0:hostname(config-ipv4_pfx)# deny 0.0.0.0/0
RP/0/RP0:hostname(config-ipv4_pfx)# exit
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# distance 10 1.0.0.0/8 target_routes
RP/0/RP0:hostname(config-isis-af)# distance 80
```

hello-interval (IS-IS)

To specify the length of time between consecutive hello packets sent by the Intermediate System-to-Intermediate System (IS-IS) protocol software, use the **hello-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

hello-interval *seconds* [**level** {**1** | **2**}]
no hello-interval [*seconds*] [**level** {**1** | **2**}]

Syntax Description

seconds	Integer value (in seconds) for the length of time between consecutive hello packets. By default, a value three times the hello interval *seconds* is advertised as the *hold time* in the hello packets sent. (That multiplier of three can be changed by using the **hello-multiplier** command.) With smaller hello intervals, topological changes are detected more quickly, but there is more routing traffic. Range is 1 to 65535 seconds.
level { **1** | **2** }	(Optional) Specifies the hello interval for Level 1 and Level 2 independently. For broadcast interfaces only.

Command Default

seconds : 10 seconds

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure TenGigE interface 0/6/0/0 to advertise hello packets every 5 seconds for Level 1 topology routes. This situation causes more traffic than configuring a longer interval, but topological changes are detected more quickly.

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/6/0/0
RP/0/RP0:hostname(config-isis-if)# hello-interval 5 level 1
```

hello-multiplier

To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the **hello-multiplier** command in interface configuration mode. To restore the default value, use the **no** form of this command.

hello-multiplier *multiplier* [**level** {**1** | **2**}]
no hello-multiplier [*multiplier*] [**level** {**1** | **2**}]

Syntax Description

multiplier	Advertised hold time in IS-IS hello packets is set to the hello multiplier times the hello interval. Range is 3 to 1000. Neighbors declare an adjacency to this down router after not having received any IS-IS hello packets during the advertised hold time. The hold time (and thus the hello multiplier and the hello interval) can be set on an individual interface basis, and can be different between different networking devices in one area. Using a smaller hello multiplier gives faster convergence, but can result in more routing instability. Increase the hello multiplier to a larger value to help network stability when needed. Never configure a hello multiplier to a value lower than the default value of 3.
level { **1** | **2** }	(Optional) Specifies the hello multiplier independently for Level 1 or Level 2 adjacencies.

Command Default

multiplier : 3

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The “holding time” carried in an IS-IS hello packet determines how long a neighbor waits for another hello packet before declaring the neighbor to be down. This time determines how quickly a failed link or neighbor is detected so that routes can be recalculated.

Use the **hello-multiplier** command in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

On point-to-point links, there is only one hello for both Level 1 and Level 2. Separate Level 1 and Level 2 hello packets are also sent over nonbroadcast multiaccess (NBMA) networks in multipoint mode, such as X.25, Frame Relay, and ATM.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how the network administrator wants to increase network stability by making sure an adjacency goes down only when many (ten) hello packets are missed. The total time to detect link failure is 60 seconds. This strategy ensures that the network remains stable, even when the link is fully congested.

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/2/0/1
RP/0/RP0:hostname(config-isis-if)# hello-interval 6
RP/0/RP0:hostname(config-isis-if)# hello-multiplier 10
```

hello-padding

To configure padding on Intermediate System-to-Intermediate System (IS-IS) hello protocol data units (IIH PDUs) for all IS-IS interfaces on the router, use the **hello-padding** command in interface configuration mode. To suppress padding, use the **no** form of this command.

hello-padding {**disable** | **sometimes**} [**level** {**1** | **2**}]
no hello-padding {**disable** | **sometimes**} [**level** {**1** | **2**}]

Syntax Description

disable	Suppresses hello padding.
sometimes	Enables hello padding during adjacency formation only.
level { **1** | **2** }	(Optional) Specifies hello padding for Level 1 or Level 2 independently.

Command Default

Hello padding is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

You might want to suppress hello padding to conserve network resources. The lower the circuit speed, the higher the percentage of padding overhead. Before suppressing the hello padding, you should know your physical and data link layer configurations and have control over them, and also know your router configuration at the network layer.

For point-to-point links, IS-IS sends only a single hello for Level 1 and Level 2, making the **level** keyword meaningless on point-to-point links. To modify hello parameters for a point-to-point interface, omit the **level** keyword.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to suppress IS-IS hello padding over local area network (LAN) circuits for interface TenGig Ethernet 0/2/0/1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/2/0/1
RP/0/RP0:hostname(config-isis-if)# hello-padding disable
```

hello-password

To configure the authentication password for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **hello-password** command in interface configuration mode. To disable authentication, use the **no** form of this command.

hello-password [{**hmac-md5** | **text**}] [{**clear** | **encrypted**}] *password* [**level** {**1** | **2**}] [**send-only**]
no hello-password [{**hmac-md5** | **text**}] [{**clear** | **encrypted**}] *password* [**level** {**1** | **2**}] [**send-only**]

Syntax Description

hmac-md5	(Optional) Specifies that the password use HMAC-MD5 authentication.
text	(Optional) Specifies that the password use clear text password authentication.
clear	(Optional) Specifies that the password be unencrypted.
encrypted	(Optional) Specifies that the password be encrypted using a two-way algorithm.
password	Authentication password you assign for an interface.
level { **1** | **2** }	(Optional) Specifies whether the password is for a Level 1 or a Level 2 protocol data unit (PDU).
send-only	(Optional) Specifies that the password applies only to protocol data units (PDUs) that are being sent and does not apply to PDUs that are being received.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

password: encrypted text

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When a **text** password is configured, it is exchanged as clear text. Therefore, the **hello-password** command provides limited security.

When an **hmac-md5** password is configured, the password is never sent over the network and is instead used to calculate a cryptographic checksum to ensure the integrity of the exchanged data.

For point-to-point links, IS-IS sends only a single hello for Level 1 and Level 2, making the **level** keyword meaningless on point-to-point links. To modify hello parameters for a point-to-point interface, omit the **level** keyword.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure a password with HMAC-MD5 authentication for hello packets running on TenGigE 0/2/0/3 interface:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/2/0/3
RP/0/RP0:hostname(config-isis-if)# hello-password hmac-md5 clear mypassword
```

hello-password accept

To configure an additional authentication password for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **hello-password accept** command in interface configuration mode. To disable authentication, use the **no** form of this command.

hello-password accept {**clear** | **encrypted**} *password* [**level** {**1** | **2**}]
no hello-password accept {**clear** | **encrypted**} *password* [**level** {**1** | **2**}]

Syntax Description

clear	Specifies that the password be unencrypted.
encrypted	Specifies that the password be encrypted using a two-way algorithm.
password	Authentication password you assign.
level { **1** | **2** }	(Optional) Specifies the password for Level 1 or Level 2 independently.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **hello-password accept** command to add an additional password for an IS-IS interface. An authentication password must be configured using the **hello-password** command before an accept password can be configured for the corresponding level.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure a password:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/2/0/3
RP/0/RP0:hostname(config-isis)# hello-password accept encrypted 111D1C1603
```

hello-password keychain

To configure the authentication password keychain for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **hello-password keychain** command in interface configuration mode. To disable the authentication password keychain, use the **no** form of this command.

hello-password keychain *keychain-name* [**level** {**1** | **2**}] [**send-only**]
no hello-password keychain *keychain-name* [**level** {**1** | **2**}] [**send-only**]

Syntax Description

keychain	Keyword that specifies the keychain to be configured. An authentication password keychain is a sequence of keys that are collectively managed and used for authenticating a peer-to-peer group.
keychain-name	Specifies the name of the keychain.
level { **1** | **2** }	(Optional) Specifies whether the keychain is for a Level 1 or a Level 2 protocol data unit (PDU).
send-only	(Optional) Specifies that the keychain applies only to protocol data units (PDUs) that are being sent and does not apply to PDUs that are being received.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

password: encrypted text

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Specify a keychain to enable keychain authentication between two IS-IS peers. Use the **keychain** *keychain-name* keyword and argument to implement hitless key rollover for authentication.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure a password keychain for level 1, send only authentication on a TenGigE interface:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-isis-if)# hello-password keychain mykeychain level 1 send-only
```

hostname dynamic disable

To disable Intermediate System-to-Intermediate System (IS-IS) routing protocol dynamic hostname mapping, use the **hostname dynamic** command in router configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

hostname dynamic disable
no hostname dynamic disable

Syntax Description

disable	Disables dynamic host naming.

Command Default

Router names are dynamically mapped to system IDs.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

In an IS-IS routing domain, each router is represented by a 6-byte hexadecimal system ID. When network administrators maintain and troubleshoot networking devices, they must know the router name and corresponding system ID.

Link-state packets (LSPs) include the dynamic hostname in the type, length, and value (TLV) which carries the mapping information across the entire domain. Every router in the network, upon receiving the TLV from an LSP, tries to install it in a mapping table. The router then uses the mapping table when it wants to convert a system ID to a router name.

To display the entries in the mapping tables, use the **show isis hostname** command.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to disable dynamic mapping of hostnames to system IDs:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# hostname dynamic disable
```

ignore-lsp-errors

To override the default setting of a router to ignore Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs) that are received with internal checksum errors, use the **ignore-lsp-errors disable** command in router configuration mode. To enable ignoring IS-IS LSP errors, use the **no** form of this command.

ignore-lsp-errors disable
no ignore-lsp-errors disable

Syntax Description

disable	Disables the functionality of the command.

Command Default

The system purges corrupt LSPs that cause the initiator to regenerate LSPs.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The IS-IS protocol definition requires that a received LSP with an incorrect data-link checksum be purged by the receiver, which causes the initiator of the packet to regenerate it. However, if a network has a link that causes data corruption and at the same time is delivering LSPs with correct data-link checksums, a continuous cycle of purging and regenerating large numbers of packets can occur. Because this situation could render the network nonfunctional, use this command to ignore these LSPs rather than purge the packets.

The receiving network devices use link-state packets to maintain their routing tables.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to instruct the router to ignore LSPs that have internal checksum errors:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# ignore-lsp-errors disable
```

interface (IS-IS)

To configure the Intermediate System-to-Intermediate System (IS-IS) protocol on an interface, use the **interface** command in router configuration mode. To disable IS-IS routing for interfaces, use the **no** form of this command.

interface *type interface-path-id*
no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

No interfaces are specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

An address family must be established on the IS-IS interface before the interface is enabled for IS-IS protocol operation.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to enable an IS-IS multitopology configuration for IPv4 on TenGigE interface 0/3/0/0:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# net 49.0000.0000.0001.00
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/3/0/0
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-if-af)# metric-style wide level 1
!
RP/0/RP0:hostname(config)# interface TenGigE 0/3/0/0
RP/0/RP0:hostname(config-if)# ipv4 address 2001::1/64
```

ispf

To configure the incremental shortest path first (iSPF) algorithm to calculate network topology, use the **ispf** command in address family configuration mode. To disable this algorithm function, use the **no** form of this command.

ispf [**level** {**1** | **2**}]
no ispf [**level** {**1** | **2**}]

Syntax Description

level { **1** | **2** }	(Optional) Configures the iSPF algorithm for Level 1 or Level 2 independently.

Command Default

The iSPF algorithm is not configured.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The iSPF algorithm may be used to reduce the processor load when IS-IS needs to recalculate its topology after minor changes.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure iSPF for the IPv4 unicast topology at Level 1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# ispf level 1
```

is-type

To configure the routing level for an Intermediate System-to-Intermediate System (IS-IS) area, use the **is-type** command in router configuration mode. To set the routing level to the default level, use the **no** form of this command.

is-type {**level-1** | **level-1-2** | **level-2-only**}
no is-type [{**level-1** | **level-1-2** | **level-2-only**}]

Syntax Description

level-1	Specifies that the router perform only Level 1 (intra-area) routing. This router learns only about destinations inside its area. Level 2 (interarea) routing is performed by the closest Level 1-2 router.
level-1-2	Specifies that the router perform both Level 1 and Level 2 routing.
level-2-only	Specifies that the routing process acts as a Level 2 (interarea) router only. This router is part of the backbone, and does not communicate with Level 1-only routers in its own area.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When the router is configured with Level 1 routing only, this router learns about destinations only inside its area. Level 2 (interarea) routing is performed by the closest Level 1-2 router.

When the router is configured with Level 2 routing only, this router is part of the backbone, and does not communicate with Level 1 routers in its own area.

The router has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone and the existence of all other areas.

We highly recommend that you configure the type of an IS-IS routing process to establish the proper level of adjacencies. If there is only one area in the network, there is no need to run both Level 1 and Level 2 routing algorithms.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to specify that the router is part of the backbone and that it does not communicate with Level 1-only routers:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# is-type level-2-only
```

log adjacency changes (IS-IS)

To cause an IS-IS instance to generate a log message when an Intermediate System-to-Intermediate System (IS-IS) adjacency changes state (up or down), use the **log adjacency changes** command in router configuration mode. To restore the default value, use the **no** form of this command.

log adjacency changes
no log adjacency changes

Command Default

No IS-IS instance log messages are generated.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **log adjacency changes** command to monitor IS-IS adjacency state changes; it may be very useful when you are monitoring large networks. Messages are logged using the system error message facility. Messages can be in either of two forms:

```
%ISIS-4-ADJCHANGE: Adjacency to 0001.0000.0008 (Gi 0/2/1/0) (L2) Up, new adjacency
%ISIS-4-ADJCHANGE: Adjacency to router-gsr8 (Gi 0/2/1/0) (L1) Down, Holdtime expired
```

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure the router to log adjacency changes:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# log adjacency changes
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

log pdu drops

To log Intermediate System-to-Intermediate System (IS-IS) protocol data units (PDUs) that are dropped, use the **log pdu drops** command in router configuration mode. To disable this function, use the **no** form of this command.

log pdu drops
no log pdu drops

Command Default

PDU logging is disabled.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **log pdu drops** command to monitor a network when IS-IS PDUs are suspected of being dropped. The reason for the PDU being dropped and current PDU drop statistics are recorded.

The following are examples of PDU logging output:

```
 %ISIS-4-ERR_IIH_INPUT_Q_OVERFLOW: IIH input queue overflow: 86 total drops; 19 IIH drops,
44 LSP drops, 23 SNP drops
 %ISIS-4-ERR_LSP_INPUT_Q_OVERFLOW: LSP input queue overflow: 17 total drops; 9 IIH drops,
3 LSP drops, 5 SNP drops
```

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to enable PDU logging:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# log pdu drops
```

lsp-interval

To configure the amount of time between consecutive link-state packets (LSPs) sent on an Intermediate System-to-Intermediate System (IS-IS) interface, use the **lsp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

lsp-interval *milliseconds* [**level** {**1** | **2**}]
no lsp-interval [*milliseconds*] [**level** {**1** | **2**}]

Syntax Description

milliseconds	Time delay (in milliseconds) between successive LSPs. Range is 1 to 4294967295.
level { **1** | **2** }	(Optional) Configures the LSP time delay for Level 1 or Level 2 independently.

Command Default

milliseconds : 33 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to cause the system to send LSPs every 100 milliseconds (10 packets per second) on Level 1 and Level 2:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/2/0/1
RP/0/RP0:hostname(config-isis-if)# lsp-interval 100
```

lsp-password

To configure the link-state packet (LSP) authentication password, use the **lsp-password** command in router configuration mode. To remove the **lsp-password** command from the configuration file and disable link-state packet authentication, use the **no** form of this command.

lsp-password [{[{**hmac-md5** | **text**}] [{**clear** | **encrypted**}] *password* | **keychain** *keychain-name*}] [**level** {**1** | **2**}] [**send-only**] [**snp send-only**]
no lsp-password [{[{**hmac-md5** | **text**}] [{**clear** | **encrypted**}] *password* | **keychain** *keychain-name*}] [**level** {**1** | **2**}] [**send-only**] [**snp send-only**]

Syntax Description

hmac-md5	Specifies that the password uses HMAC-MD5 authentication.
text	Specifies that the password uses clear text password authentication.
clear	Specifies that the password be unencrypted.
encrypted	Specifies that the password be encrypted using a two-way algorithm.
password	Authentication password you assign.
keychain	(Optional) Specifies a keychain.
keychain-name	Name of the keychain.
level { **1** | **2** }	(Optional) Specifies the password for Level 1 or Level 2 independently.
send-only	(Optional) Adds passwords to LSP and sequence number protocol (SNP) data units when they are sent. Does not check for authentication in received LSPs or sequence number PDUs (SNPs).
snp send-only	(Optional) Adds passwords to SNP data units when they are sent. Does not check for authentication in received SNPs. This option is available when the **text** keyword is specified.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When a **text** password is configured, it is exchanged as clear text. Therefore, the **lsp-password** command provides limited security.

When an **HMAC-MD5** password is configured, the password is never sent over the network and is instead used to calculate a cryptographic checksum to ensure the integrity of the exchanged data.

The recommended password configuration is that both incoming and outgoing SNPs be authenticated.

Note To disable SNP password checking, the **snp send-only** keywords must be specified in the **lsp-password** command.

To configure an additional password, use the **lsp-password accept** command.

Specify a key chain to enable key chain authentication between two IS-IS peers. Use the **keychain** *keychain-name* keyword and argument to implement hitless key rollover for authentication.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure separate Level 1 and Level 2 LSP and SNP passwords, one with HMAC-MD5 authentication and encryption and one with clear text password authentication and no encryption:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# lsp-password hmac-md5 clear password1 level 1
RP/0/RP0:hostname(config-isis)# lsp-password text clear password2 level 2
```

lsp-password accept

To configure an additional link-state packet (LSP) authentication password, use the **lsp-password accept** command in router configuration mode. To remove the **lsp-password accept** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

lsp-password accept {**clear** | **encrypted**} *password* [**level** {**1** | **2**}]
no lsp-password accept [{**clear** | **encrypted**} *password* [**level** {**1** | **2**}]]

Syntax Description

clear	Specifies that the password be unencrypted.
encrypted	Specifies that the password be encrypted using a two-way algorithm.
password	Authentication password you assign.
level { **1** | **2** }	(Optional) Specifies the password for Level 1 or Level 2 independently.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **lsp-password accept** command adds an additional password for use when the system validates incoming LSPs and sequence number PDUs (SNPs). An LSP password must be configured using the **lsp-password** command before an accept password can be configured for the corresponding level.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure a Level 1 LSP and SNP password:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# lsp-password accept encrypted password1 level 1
```

lsp-refresh-interval

To set the time between regeneration of link-state packets (LSPs) that contain different sequence numbers, use the **lsp-refresh-interval** command in router configuration mode. To restore the default refresh interval, use the **no** form of this command.

lsp-refresh-interval *seconds* [**level** {**1** | **2**}]
no lsp-refresh-interval [*seconds* [**level** {**1** | **2**}]]

Syntax Description

seconds	Refresh interval (in seconds). Range is 1 to 65535 seconds.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

seconds : 900 seconds (15 minutes)

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The refresh interval determines the rate at which the software periodically sends the route topology information that it originates. This behavior is done to keep the information from becoming too old. By default, the refresh interval is 900 seconds (15 minutes).

LSPs must be refreshed periodically before their lifetimes expire. The refresh interval must be less than the LSP lifetime specified with this router command. Reducing the refresh interval reduces the amount of time that undetected link-state database corruption can persist at the cost of increased link utilization. (This event is extremely unlikely, however, because there are other safeguards against corruption.) Increasing the interval reduces the link utilization caused by the flooding of refreshed packets (although this utilization is very small).

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to change the LSP refresh interval to 10,800 seconds (3 hours):

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# lsp-refresh-interval 10800
```

maximum-paths (IS-IS)

To configure the maximum number of parallel routes that an IP routing protocol will install the routing table, use the **maximum-paths** command in address family configuration mode. To remove the **maximum-paths** command from the configuration file and restore the system default behavior, use the **no** form of this command. By default up to 8 parallel ECMP paths are used by IS-IS routing protocol.

maximum-paths *maximum*
no maximum-paths

Syntax Description

maximum	Maximum number of parallel routes that IS-IS can install in a routing table.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to allow a maximum of 16 paths to a destination:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# maximum-paths 16
```

maximum-redistributed-prefixes (IS-IS)

To specify an upper limit on the number of redistributed prefixes (subject to summarization) that the Intermediate System-to-Intermediate System (IS-IS) protocol advertises, use the **maximum-redistributed-prefixes** command in address family mode. To disable this feature, use the **no** form of this command.

maximum-redistributed-prefixes *maximum* [**level** {**1** | **2**}]
no maximum-redistributed-prefixes [*maximum* [**level** {**1** | **2**}]]

Syntax Description

maximum	Maximum number of redistributed prefixes advertised. Range is 1 to 28000.
level { **1** | **2** }	(Optional) Specifies maximum prefixes for Level 1 or Level 2.

Command Default

maximum: 10000

level : 1-2

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **maximum-redistributed-prefixes** command to prevent a misconfiguration from resulting in redistribution of excess prefixes. If IS-IS encounters more than the maximum number of prefixes, it sets a bi-state alarm. If the number of to-be-redistributed prefixes drops back to the maximum or lower—either through reconfiguration or a change in the redistribution source—IS-IS clears the alarm.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to specify the number of redistributed prefixes at 5000 for Level 2:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# maximum-redistributed-prefixes 5000 level 2
```

max-lsp-lifetime

To set the maximum time that link-state packets (LSPs) persist without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default time, use the **no** form of this command.

max-lsp-lifetime *seconds* [**level** {**1** | **2**}]
no max-lsp-lifetime [*seconds* [**level** {**1** | **2**}]]

Syntax Description

seconds	Lifetime (in seconds) of the LSP. Range from 1 to 65535 seconds.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

seconds : 1200 seconds (20 minutes)

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval** command. The maximum LSP lifetime must be greater than the LSP refresh interval.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to set the maximum time that the LSP persists to 11,000 seconds (more than 3 hours):

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# max-lsp-lifetime 11000
```

max-link-metric

max-link-metric [**level 1 | 2**]
no max-link-metric [**level 1 | 2**]

Syntax Description

max-link-metric	Specifies maximum metrics for NLRIs during router overload. If specified with a level number, the maximum link metric is applied only across links for the specified level. If specified without a level number, the maximum link metric is applied across all levels.

Command Default

Maximum metric is disabled.

Command Modes

IS-IS configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When a router is configured with the IS-IS overload bit, it participates in the routing process when the overload bit is set, but does not forward traffic (except for traffic to directly connected interfaces). By configuring the **max-metric-link** statement, the overloaded router is used as a transit node of last resort.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to enable maximum metric on a router:

```
RP/0/RP0:hostname(config)# router isis ring
RP/0/RP0:hostname(config-isis)# max-link-metric
RP/0/RP0:hostname(config-isis)# exit
RP/0/RP0:hostname(config)#
```

mesh-group (IS-IS)

To optimize link-state packet (LSP) flooding in highly meshed networks, use the **mesh-group** command in interface configuration mode. To remove a subinterface from a mesh group, use the **no** form of this command.

mesh-group {*number* | **blocked**}
no mesh-group

Syntax Description

number	Number identifying the mesh group of which this interface is a member. Range is 1 to 4294967295.
blocked	Specifies that no LSP flooding takes place on this interface.

Command Default

There is no mesh group configuration (normal LSP flooding).

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

LSPs first received on subinterfaces that are not part of a mesh group are flooded to all other subinterfaces in the usual way.

LSPs first received on subinterfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group. If the **blocked** keyword is configured on a subinterface, then a newly received LSP is not flooded out over that interface.

To minimize the possibility of incomplete flooding, you should allow unrestricted flooding over at least a minimal set of links in the mesh. Selecting the smallest set of logical links that covers all physical paths results in very low flooding, but less robustness. Ideally you should select only enough links to ensure that LSP flooding is not detrimental to scaling performance, but enough links to ensure that under most failure scenarios, no router is logically disconnected from the rest of the network. In other words, blocking flooding on all links permits the best scaling performance, but there is no flooding. Permitting flooding on all links results in very poor scaling performance.

Task ID

Task ID	Operations
isis	read, write

Examples

In the following example, six interfaces are configured in three mesh groups. LSPs received are handled as follows:

- LSPs first received by TenGigE interface 0/1/0/0 are flooded to all interfaces except TenGigE0/1/0/1 (which is part of the same mesh group) and TenGigE0/3/0/0 (which is blocked).
- LSPs first received by TenGigE0/2/0/1 are flooded to all interfaces except TenGigE0/2/0/0 (which is part of the same mesh group) and TenGigE0/3/0/0 (which is blocked).

- LSPs first received by TenGigE0/3/0/0 are not ignored, but flooded as usual to all interfaces.
- LSPs received first through TenGigE0/3/0/1 are flooded to all interfaces, except TenGigE0/3/0/0 (which is blocked).

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-isis-if)# mesh-group 10
RP/0/RP0:hostname(config-isis-if)# exit
RP/0/RP0:hostname(config-isis)# interface TenGigE0/1/0/1
RP/0/RP0:hostname(config-isis-if)# mesh-group 10
RP/0/RP0:hostname(config-isis-if)# exit
RP/0/RP0:hostname(config-isis)# interface TenGigE0/2/0/0
RP/0/RP0:hostname(config-isis-if)# mesh-group 11
RP/0/RP0:hostname(config-isis-if)# exit
RP/0/RP0:hostname(config-isis)# interface TenGigE0/2/0/1
RP/0/RP0:hostname(config-isis-if)# mesh-group 11
RP/0/RP0:hostname(config-isis-if)# exit
RP/0/RP0:hostnameconfig-isis)# interface TenGigE0/3/0/1
RP/0/RP0:hostname(config-isis-if)# mesh-group 12
RP/0/RP0:hostname(config-isis-if)# exit
RP/0/RP0:hostname(config-isis)# interface TenGigE0/3/0/0
RP/0/RP0:hostname(config-isis-if)# mesh-group blocked
```

metric (IS-IS)

To configure the metric for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **metric** command in address family or interface address family configuration mode. To restore the default metric value, use the **no** form of this command.

metric {*default-metric* | **maximum**} [**level** {**1** | **2**}]
no metric [{*default-metric* | **maximum**} [**level** {**1** | **2**}]]

Syntax Description

default-metric	Metric assigned to the link and used to calculate the cost from each other router using the links in the network to other destinations. Range is 1 to 63 for narrow metric and 1 to 16777214 for wide metric. **Note** Setting the default metric under address family results in setting the same metric for all interfaces that is associated with the address family. Setting a metric value under an interface overrides the default metric
maximum	Specifies maximum wide metric. All routers exclude this link from their shortest path first (SPF).
level { **1** | **2** }	(Optional) Specifies the SPF calculation for Level 1 or Level 2 independently.

Command Default

default-metric : Default is 10.

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Address family configuration

Interface address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Specifying the **level** keyword resets the metric only for the specified level. We highly recommend that you configure metrics on all interfaces.

Set the default metric under address family to set the same metric for all interfaces that is associated with the address family. Set a metric value under an interface to override the default metric.

We highly recommend that you configure metrics on all interfaces.

Metrics of more than 63 cannot be used with narrow metric style.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure Packet-over-SONET/SDH 0/1/0/1 interface with a default link-state metric cost of 15 for Level 1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/1/0/1
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-if-af)# metric 15 level 1
```

The following example shows how to configure a metric cost of 15 for all interfaces under address family IPv4 unicast for level 2:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# metric 15 level 2
```

metric-style narrow

To configure the Intermediate System-to-Intermediate System (IS-IS) software to generate and accept old-style type, length, and value (TLV) objects, use the **metric-style narrow** command in address family configuration mode. To remove the **metric-style narrow** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

metric-style narrow [**transition**] [**level** {**1** | **2**}]
no metric-style narrow [**transition**] [**level** {**1** | **2**}]

Syntax Description

transition	(Optional) Instructs the router to generate and accept both old-style and new-style TLV objects. It generates only old-style TLV objects.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

Old-style TLVs are generated.

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

IS-IS traffic engineering extensions include new-style TLV objects with wider metric fields than old-style TLV objects. By default, the router generates old-style TLV objects only. To perform Multiprotocol Label Switching traffic engineering (MPLS TE), a router must generate new-style TLV objects.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure the router to generate and accept only old-style TLV objects on router Level 1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# metric-style narrow level 1
```

metric-style transition

To configure the Intermediate System-to-Intermediate System (IS-IS) software to generate and accept both old-style and new-style type, length, and value (TLV) objects, use the **metric-style transition** command in address family configuration mode. To remove the **metric-style transition** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

metric-style transition [**level** {**1** | **2**}]
no metric-style transition [**level** {**1** | **2**}]

Syntax Description

transition	Instructs the router to generate and accept both old-style and new-style TLV objects.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

Old-style TLVs are generated, if this command is not configured.

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

IS-IS traffic engineering extensions include new-style TLV objects which have wider metric fields than old-style TLV objects. By default, the router generates old-style TLV objects only. To perform Multiprotocol Label Switching traffic engineering (MPLS TE), a router needs to generate new-style TLV objects.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure the router to generate and accept both old-style and new-style TLV objects on Level 2:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# metric-style transition level 2
```

metric-style wide

To configure the Intermediate System-to-Intermediate System (IS-IS) software to generate and accept only new-style type, length, and value (TLV) objects, use the **metric-style wide** command in address family configuration mode. To remove the **metric-style wide** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

metric-style wide [**transition**] [**level** {**1** | **2**}]
no metric-style wide [**transition**] [**level** {**1** | **2**}]

Syntax Description

transition	(Optional) Instructs the router to generate and accept both old-style and new-style TLV objects. It generates only new-style TLV objects.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

Old-style TLV lengths are generated, if this command is not configured.

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

IS-IS traffic engineering extensions include new-style TLV objects with wider metric fields than old-style TLV objects. If you enter the **metric-style wide** command, a router generates and accepts only new-style TLV objects. Therefore, the router uses less memory and fewer other resources rather than generating both old-style and new-style TLV objects.

To perform MPLS traffic engineering, a router needs to generate new-style TLV objects.

Note This discussion of metric styles and transition strategies is oriented toward traffic engineering deployment. Other commands and models might be appropriate if the new-style TLV objects are desired for other reasons. For example, a network may require wider metrics, but might not use traffic engineering.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure a router to generate and accept only new-style TLV objects on Level 1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# metric-style wide level 1
```

microloop avoidance

Avoids micro-loops by delaying the convergence of all or protected prefixes.

To disable this function, use the **no** form of this command.

microloop avoidance [**protected** | **rib-update-delay***delay*]
no microloop avoidance

Syntax Description

(none)	Delays convergence of all prefixes.
protected	(Optional) Delays convergence of protected prefixes..
rib-update-delay *delay*	(Optional) Delays convergence of all prefixes and updates RIB after the configured delay. The range is 1 to 60000 milliseconds.

Command Default

Micro-loop avoidance is disabled by default.

Command Modes

Router isis configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When the network converges after a link failure restoration, micro-loops can form due to inconsistencies in the forwarding tables of different routers. By delaying the convergence of prefixes, you can avoid the formation of micro-loops.

You can delay the convergence of all or protected prefixes by using the **microloop avoidance** command. When configured, the command applies to all prefixes by default. To enable it for only protected prefixes, use the **protected** option.

You can delay updates to the RIB, by using the **rib-update-delay** option.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure micro-loop avoidance with IS-IS:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router isis 50
RP/0/RP0:hostname(config-isis)#microloop avoidance rib-update-delay 400
```

min-lsp-arrivaltime

To control the rate of incoming LSPs (link-state packets) LSPs, use the **min-lsp-arrivaltime** command in router configuration mode. To remove this function use the **no** form of this command.

min-lsp-arrivaltime [**initial-wait initial**] [**secondary-wait secondary**] [**maximum-wait maximum**] [**level** {**1** | **2**}]
no min-lsp-arrivaltime [**initial-wait initial**] [**secondary-wait secondary**] [**maximum-wait maximum**] [**level** {**1** | **2**}]

Syntax Description

initial-wait initial	Initial LSP calculation delay (in milliseconds). Range is 0 to 120000.
secondary-wait *secondary*	Hold time between the first and second LSP calculations (in milliseconds). Range is 0 to 120000.
maximum-wait *maximum*	Maximum interval (in milliseconds) between two consecutive LSP calculations. Range is 0 to 120000.
level { **1	2** }	(Optional) Enables the LSP interval configuration for Level 1 or Level 2 independently.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command can be used to protect a router against the possible instability of its neighbor's LSPs.

The command parameters are similair to **lsp-gen-interval**command and neighbors lsp-gen-interval values can be used to set the **min-lsp-arrivaltime**

Note The initial-wait of minimum-lsp-arrival has no use in computing maximum counts and maximum window sizes of the LSP arrival time parameter.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure min-lsp-arrival time commands:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config)# router isis isp min-lsp-arrivaltime
RP/0/RP0:hostname(config)# router isis 1 min-  lsp-arrivaltime initial-wait
RP/0/RP0:hostname(config)#router isis 1 min-lsp-arrivaltime maximum-wait
RP/0/RP0:hostname(config)#router isis 1 min-lsp-arrivaltime secondary-wait
```

mpls traffic-eng (IS-IS)

To configure a router running the Intermediate System-to-Intermediate System (IS-IS) protocol to flood Multiprotocol Label Switching traffic engineering (MPLS TE) link information into the indicated IS-IS level, use the **mpls traffic-eng** command in IPv4 address family configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng {**level-1** | **level-1-2** | **level-2-only**}
no mpls traffic-eng [{**level-1** | **level-1-2** | **level-2-only**}]

Syntax Description

level-1	Specifies routing level 1.
level-1-2	Specifies routing levels 1 and 2.
level-2-only	Specifies routing level 2.

Command Default

Flooding is disabled.

Command Modes

IPv4 address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **mpls traffic-eng** command, which is part of the routing protocol tree, to flood link resource information (such as available bandwidth) for appropriately configured links in the link-state packet (LSP) of the router.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to turn on MPLS traffic engineering for IS-IS level 1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# mpls  traffic-eng level-1
```

mpls traffic-eng multicast-intact (IS-IS)

To enable multicast-intact for Intermediate System-to-Intermediate System (IS-IS) routes with Protocol-Independent Multicast (PIM) and Multiprotocol Label Switching (MPLS) traffic engineering, use the **mpls traffic-eng multicast-intact** command in IPv4 address family configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng multicast-intact
no mpls traffic-eng [**multicast-intact**]

Syntax Description

This command has no keywords or arguments.

Command Default

Multicast-intact is disabled.

Command Modes

IPv4 address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If Multiprotocol Label Switching Traffic Engineering (MPLS-TE) is configured through the IS-IS routing domain and multicast protocols (like Protocol Independent Multicast [PIM]) are also enabled, then use the **mpls traffic-end multicast-intact** command to install nontraffic engineering next hops in the Routing Information Base (RIB) for use by multicast. The installation of IP-only next hops is in addition to the installation of the standard set of paths for a prefix, which might be through traffic engineered tunnels.

The **mpls traffic-eng multicast-intact** command allows PIM to use the native hop-by-hop neighbors even though the unicast routing is using MPLS TE tunnels.

Examples

The following example shows how to enable the multicast-intact feature:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# mpls  traffic-engmulticast-intact
```

mpls traffic-eng path-selection ignore overload

To ensure that label switched paths (LSPs) are not disabled when routers have the Intermediate System-to-Intermediate System (IS-IS) overload bit set, use the **mpls traffic-eng path-selection ignore overload** command. To disable this override, use the **no** form of this command.

mpls traffic-eng path-selection ignore overload
no mpls traffic-eng path-selection ignore overload

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When the IS-IS overload bit avoidance feature is activated, which means that they are still available for use label switched paths (LSPs), all nodes with the overload bit set, including the following nodes, are ignored:

- head nodes
- mid nodes
- tail nodes

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to activate IS-IS overload bit avoidance:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng path-selection ignore overload
```

The following example shows how to deactivate IS-IS overload bit avoidance:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# no mpls traffic-eng path-selection ignore overload
```

mpls traffic-eng router-id (IS-IS)

To specify the Multiprotocol Label Switching traffic engineering (MPLS TE) router identifier for the node, use the **mpls traffic-eng router-id** command in IPv4 address family configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng router-id {*ip-address* | *type interface-path-id*}
no mpls traffic-eng [**router-id**]

Syntax Description

ip-address	IP address in four-part, dotted-decimal notation.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

Global router identifier is used.

Command Modes

IPv4 address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The identifier of the router acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all 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 ID of the destination node, because that is the address used by the traffic engineering topology database at the tunnel head for its path calculation.

Note We recommend that loopback interfaces be used for MPLS TE, because they are more stable than physical interfaces.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with loopback interface 0:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# mpls traffic-eng router-id Loopback0
```

nsf (IS-IS)

To enable nonstop forwarding (NSF) on the next restart, use the **nsf** command in router configuration mode. To restore the default setting, use the **no** form of this command.

nsf {**cisco** | **ietf**}
no nsf {**cisco** | **ietf**}

Syntax Description

cisco	Specifies Cisco-proprietary NSF restart.
ietf	Specifies Internet Engineering Task Force (IETF) NSF restart.

Command Default

NSF is disabled.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

NSF allows an Intermediate System-to-Intermediate System (IS-IS) instance to restart using checkpointed adjacency and link-state packet (LSP) information, and to perform restart with no impact on its neighbor routers. In other words, there is no impact on other routers in the network due to the destruction and recreation of adjacencies and the system LSP.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to enable Cisco proprietary NSF:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# nsf cisco
```

nsf interface-expires

To configure the number of resends of an acknowledged nonstop forwarding (NSF)-restart acknowledgment, use the **nsf interface-expires** command in router configuration mode. To restore the default value, use the **no** form of this command.

nsf interface-expires *number*
no nsf interface-expires

Syntax Description

number	Number of resends. Range is 1 to 3.

Command Default

number : 3 resends

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When a hello packet sent with the NSF restart flag set is not acknowledged, it is re-sent. Use the **nsf interface-expires** command to control the number of times the NSF hello is re-sent. When this limit is reached on an interface, any neighbor previously known on that interface is assumed to be down and the initial shortest path first (SPF) calculation is permitted, provided that all other necessary conditions are met.

The total time period available for adjacency reestablishment (interface-timer * interface-expires) should be greater than the expected total NSF restart time.

The **nsf interface-expires** command applies only to Internet Engineering Task Force (IETF)-style NSF. It has no effect if Cisco-proprietary NSF is configured.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to allow only one retry attempt on each interface if an IETF NSF restart signal is not acknowledged:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# nsf ietf
RP/0/RP0:hostname(config-isis)# nsf interface-expires 1
```

nsf interface-timer

To configure the time interval after which an unacknowledged Internet Engineering Task Force (IETF) nonstop forwarding (NSF) restart attempt is repeated, use the **nsf interface-timer** command in router configuration mode. To restore the default value, use the **no** form of this command.

nsf interface-timer *seconds*
no nsf interface-timer

Syntax Description

seconds	NSF restart time interval (in seconds). Range is 3 to 20 seconds.

Command Default

seconds : 10 seconds

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When the IETF NSF restart process begins, hello packets send an NSF restart flag that must be acknowledged by the neighbors of the router. Use the **nsf interface-timer** command to control the restart time interval after the hello packet is re-sent. The restart time interval need not match the hello interval.

The **nsf interface-timer** command applies only to IETF-style NSF. It has no effect if Cisco proprietary NSF is configured.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to ensure that a hello packet with the NSF restart flag set is sent again every 5 seconds until the flag is acknowledged:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# nsf ietf
RP/0/RP0:hostname(config-isis)# nsf interface-timer 5
```

nsf lifetime (IS-IS)

To configure the maximum route lifetime following a nonstop forwarding (NSF) restart, use the **nsf lifetime** command in router configuration mode. To restore the default value, use the **no** form of this command.

nsf lifetime *seconds*
no nsf lifetime

Syntax Description

seconds	Maximum route lifetime (in seconds) following an NSF restart. Range is 5 to 300 seconds.

Command Default

seconds : 60 seconds (1 minute)

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **nsf lifetime** command to set the maximum available time for the reacquisition of checkpointed adjacencies and link-state packets (LSPs) during a Cisco proprietary NSF restart. LSPs and adjacencies not recovered during this time period are abandoned, thus causing changes to the network topology.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure the router to allow only 20 seconds for the entire NSF process:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# nsf cisco
RP/0/RP0:hostname(config-isis)# nsf lifetime 20
```

passive (IS-IS)

To suppress Intermediate System-to-Intermediate System (IS-IS) packets from being transmitted to the interface and received packets from being processed on the interface, use the **passive** command in interface configuration mode. To restore IS-IS packets coming to an interface, use the **no** form of this command.

passive
no passive

Command Default

Interface is active.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure the router to suppress IS-IS packets on TenGigE interface 0/1/0/1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/1/0/1
RP/0/RP0:hostname(config-isis-if)# passive
```

point-to-point

To configure a network of only two networking devices that use broadcast media and the integrated Intermediate System-to-Intermediate System (IS-IS) routing protocol to function as a point-to-point link instead of a broadcast link, use the **point-to-point** command in interface configuration mode. To disable the point-to-point usage, use the **no** form of this command.

point-to-point
no point-to-point

Syntax Description

This command has no keywords or arguments.

Command Default

Interface is treated as broadcast if connected to broadcast media.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **point-to-point** command only on broadcast media in a network with two networking devices. The command causes the system to issue packets point-to-point rather than as broadcasts. Configure the command on both networking devices in the network.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure a 10-Gb Ethernet interface to act as a point-to-point interface:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/6/0/0
RP/0/RP0:hostname(config-isis-if)# point-to-point
```

priority (IS-IS)

To configure the priority of designated routers, use the **priority** command in interface configuration mode. To reset the default priority, use the **no** form of this command.

priority *value* [**level** {**1** | **2**}]
no priority [*value*] [**level** {**1** | **2**}]

Syntax Description

value	Priority of a router. Range is 0 to 127.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

value : 64

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Priorities can be configured for Level 1 and Level 2 independently. Specifying Level 1 or Level 2 resets priority only for Level 1 or Level 2 routing, respectively. Specifying no level allows you to configure all levels.

The priority is used to determine which router on a LAN is the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority becomes the DIS.

In the Intermediate System-to-Intermediate System (IS-IS) protocol, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes online, it takes over the role from the current DIS. For equal priorities, the higher MAC address breaks the tie.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to give Level 1 routing priority by setting the priority level to 80. This router is now more likely to become the DIS.

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE0/6/0/0
RP/0/RP0:hostname(config-isis-if)# priority 80 level 1
```

propagate level

To propagate routes from one Intermediate System-to-Intermediate System (IS-IS) level into another level, use the **propagate level** command in address family configuration mode. To disable propagation, use the **no** form of this command.

propagate level {**1** | **2**} **into level** {**1** | **2**} **route-policy** *route-policy-name*
no propagate level {**1** | **2**} **into level** {**1** | **2**}

Syntax Description

level { **1** | **2** }	Propagates from routing Level 1 or Level 2 routes.
into	Propagates from Level 1 or Level 2 routes into Level 1 or Level 2 routes.
route-policy *route-policy-name*	Specifies a configured route policy.

Command Default

Route leaking (Level 2 to Level 1) is disabled.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

In general, route propagation from Level 1 to Level 2 is automatic. You might want to use this command to better control which Level 1 routes can be propagated into Level 2.

Propagating Level 2 routes into Level 1 is called *route leaking*. Route leaking is disabled by default. That is, Level 2 routes are not automatically included in Level 1 link-state packets (LSPs). If you want to leak Level 2 routes into Level 1, you must enable that behavior by using this command.

Propagation from Level 1 into Level 1 and from Level 2 into Level 2 is not allowed.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to redistribute Level 2 routes to Level 1:

```
  RP/0/RP0:hostname(config)# ipv4 access-list 101 permit ip 10.0.0.0 255.0.0.0 10.1.0.1
0.255.255.255
  RP/0/RP0:hostname(config)# router isis isp
  RP/0/RP0:hostname(config-isis)# net 49.1234.2222.2222.2222.00
  RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
  RP/0/RP0:hostname(config-isis-af)# propagate level 2 into level 1 route-policy policy_a
```

redistribute (IS-IS)

To redistribute routes from one routing protocol into Intermediate System-to-Intermediate System (IS-IS), use the **redistribute** command in address family configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

Border Gateway Protocol (BGP)
redistribute bgp *process-id* [{**level-1** | **level-2** | **level-1-2**}] [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-policy** *route-policy-name*]
no redistribute

Connected Routes
redistribute connected [{**level-1** | **level-2** | **level-1-2**}] [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-policy** *route-policy-name*]
no redistribute

Intermediate System-to-Intermediate System (IS-IS)
redistribute isis *process-id* [{**level-1** | **level-2** | **level-1-2**}] [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-policy** *route-policy-name*]
no redistribute

Open Shortest Path First (OSPF)
redistribute ospf *process-id* [{**level-1** | **level-2** | **level-1-2**}] [**match** {**external** [{**1** | **2**}] | **internal** | **nssa-external** [{**1** | **2**}]}] [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-policy** *route-policy-name*]
no redistribute

Static Routes
redistribute static [{**level-1** | **level-2** | **level-1-2**}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *route-policy-name*]
no redistribute

Syntax Description

process-id	For the **bgp** keyword, an autonomous system number has the following ranges: • Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. • Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. • Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535. For the **isis** keyword, an IS-IS instance identifier from which routes are to be redistributed. For the **ospf** keyword, an OSPF process name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
level-1	(Optional) Specifies that redistributed routes are advertised in the Level-1 LSP of the router.

level-1-2	(Optional) Specifies that redistributed routes are advertised in the Level-1-2 LSP of the router.
level-2	(Optional) Specifies that redistributed routes are advertised in the Level-2 LSP of the router.
metric *metric-value*	(Optional) Specifies the metric used for the redistributed route. Range is 0 to 16777215. The *metric-value* must be consistent with the IS-IS metric style of the area and topology into which the routes are being redistributed.
route-policy *route-policy-name*	(Optional) Specifies the identifier of a configured policy. A policy is used to filter the importation of routes from this source routing protocol to IS-IS.
match { **internal** | **external** [**1** | **2**] | **nsaa-external** [**1** | **2**]}	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one or more of the following: • **internal** —Routes that are internal to a specific autonomous system (intra- and interarea OSPF routes). • **external** [**1 | 2**]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • **nssa-external** [**1 | 2**]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 not-so-stubby area (NSSA) external routes. For the **external** and **nssa-external** options, if a type is not specified, then both Type 1 and Type 2 are assumed.

Command Default

Level 2 is configured if no level is specified.

metric-type: internal

match : If no match keyword is specified, all OSPF routes are redistributed.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

In this example, IS-IS instance isp_A readvertises all of the routes of IS-IS instance isp_B in Level 2 LSP. Note that the **level-2** keyword affects which levels instance isp_A advertises the routes in and has no impact on which routes from instance isp_B are advertised. (Any Level 1 routes from IS-IS instance isp_B are included in the redistribution.

```
RP/0/RP0:hostname(config)# router isis isp_A
RP/0/RP0:hostname(config-isis)# net 49.1234.2222.2222.2222.00
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# redistribute isis isp_B level-2
!
RP/0/RP0:hostname(config)# router isis isp_B
RP/0/RP0:hostname(config-isis)# is-type level 1
RP/0/RP0:hostname(config-isis)# net 49.4567.2222.2222.2222.00
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
```

retransmit-interval (IS-IS)

To configure the amount of time between retransmission of each Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) on a point-to-point link, use the **retransmit-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

retransmit-interval *seconds* [**level** {**1** | **2**}]
no retransmit-interval [*seconds* [**level** {**1** | **2**}]]

Syntax Description

seconds	Time (in seconds) between consecutive retransmissions of each LSP. It is an integer that should be greater than the expected round-trip delay between any two networking devices on the attached network. Range is 0 to 65535 seconds.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

seconds : 5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **retransmit-interval** command has no effect on LAN (multipoint) interfaces. On point-to-point links, the value can be increased to enhance network stability.

Because retransmissions occur only when LSPs are dropped, setting this command to a higher value has little effect on reconvergence. The more neighbors networking devices have, and the more paths over which LSPs can be flooded, the higher this value can be made.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure TenGigE interface 0/2/0/1 for retransmission of IS-IS LSPs every 60 seconds for a large serial line:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/2/0/1
RP/0/RP0:hostname(config-isis-if)# retransmit-interval 60
```

retransmit-throttle-interval

To configure minimum interval between retransmissions of different Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs) on a point-to-point interface, use the **retransmit-throttle-interval** command in interface configuration mode. To remove the command from the configuration file and restore the system to its default condition, use the **no** form of this command.

retransmit-throttle-interval *milliseconds* [**level** {**1** | **2**}]
no retransmit-throttle-interval [*milliseconds* [**level** {**1** | **2**}]]

Syntax Description

milliseconds	Minimum delay (in milliseconds) between LSP retransmissions on the interface. Range is 0 to 65535.
level { **1** | **2** }	(Optional) Specifies routing Level 1 or Level 2 independently.

Command Default

Default is 0.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **retransmit-throttle-interval** command to define the minimum period of time that must elapse between retransmitting any two consecutive LSPs on an interface. The **retransmit-throttle-interval** command may be useful in very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic. This command controls the rate at which LSPs can be re-sent on the interface.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure TenGigE interface 0/2/0/1 to limit the rate of LSP retransmissions to one every 300 milliseconds:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/2/0/1
RP/0/RP0:hostname(config-isis-if)# retransmit-throttle-interval 300
```

router isis

To enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS instance, use the **router isis** command. To disable IS-IS routing, use the **no** form of this command.

router isis *instance-id*
no router isis *instance-id*

Syntax Description

instance-id	Name of the routing process. Maximum number of characters is 40.

Command Default

An IS-IS routing protocol is not enabled.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **router isis** command to create an IS-IS routing process. An appropriate network entity title (NET) must be configured to specify the address of the area (Level 1) and system ID of the router. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible.

Multiple IS-IS processes can be configured. Up to eight processes are configurable. A maximum of five IS-IS instances on a system are supported.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure IS-IS for IP routing:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# net 49.0001.0000.0001.00
```

set-overload-bit

To configure the router to signal other routers not to use it as an intermediate hop in their shortest path first (SPF) calculations, use the **set-overload-bit** command in router configuration mode. To remove the designation, use the **no** form of this command.

set-overload-bit [**on-startup** {*delay* | **wait-for-bgp**}] [**level** {**1** | **2**}] [**advertise** {**external** | **interlevel**}]
no set-overload-bit [**on-startup** {*delay* | **wait-for-bgp**}] [**level** {**1** | **2**}] [**advertise** {**external** | **interlevel**}]

Syntax Description

on-startup	(Optional) Sets the overload bit only temporarily after reboot.
delay	(Optional) Time (in seconds) to advertise when the router is overloaded after reboot. Range is 5 to 86400 seconds (86400 seconds = 1 day).
wait-for-bgp	(Optional) Sets the overload bit on startup until the Border Gateway Protocol (BGP) signals converge or time out.
level { **1** | **2** }	(Optional) Specifies the overload bit for Level 1 or Level 2 independently.
advertise { **external** | **interlevel**	(Optional) Sets the overload bit set if the router advertises the following types of IP prefixes: • **external**—If overload-bit set advertises IP prefixes learned from other protocols • **interlevel**— If overload-bit set advertise IP prefixes learned from another ISI S level

Command Default

The overload bit is not set.

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **set-overload-bit** command to force the router to set the overload bit in its nonpseudonode link-state packets (LSPs). Normally the setting of the overload bit is allowed only when a router experiences problems. For example, when a router is experiencing a memory shortage, the reason might be that the link-state database is not complete, resulting in an incomplete or inaccurate routing table. If the overload bit is set in the LSPs of the unreliable router, other routers can ignore the router in their SPF calculations until it has recovered from its problems. The result is that no paths through the unreliable router are seen by other routers in the Intermediate System-to-Intermediate System (IS-IS) area. However, IP prefixes directly connected to this router are still reachable.

The **set-overload-bit** command can be useful when you want to connect a router to an IS-IS network, but do not want real traffic flowing through it under any circumstances.

Routers with overload bit set are:

- A test router in the lab, connected to a production network.
- A router configured as an LSP flooding server, for example, on a nonbroadcast multiaccess (NBMA) network, in combination with the mesh group feature.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure the overload bit:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# set-overload-bit
```

set-attached-bit

To configure an Intermediate System-to-Intermediate System (IS-IS) instance with an attached bit in the Level 1 link-state packet (LSP), use the **set-attached-bit** command in address family configuration mode. To remove the **set-attached-bit** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

set-attached-bit
no set-attached-bit

Command Default

Attached bit is not set in the LSP.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **set-attached bit** command to set an IS-IS instance with an attached bit in the Level 1 LSP that allows another IS-IS instance to redistribute Level 2 topology. The attached bit is used when the Level 2 connectivity from another IS-IS instance is advertised by the Level 1 attached bit.

Cisco IOS XR software does not support multiple Level 1 areas in a single IS-IS routing instance. But the equivalent functionality is achieved by redistribution of routes between two IS-IS instances.

The attached bit is configured for a specific address family only if the **single-topology** command is not configured.

Note If connectivity for the Level 2 instance is lost, the attached bit in the Level 1 instance LSP continues sending traffic to the Level 2 instance and causes the traffic to be dropped.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to set the attached bit for a Level 1 instance that allows the Level 2 instance to redistribute routes from the Level 1 instance:

```
RP/0/RP0:hostname(config)# router isis 1
RP/0/RP0:hostname(config-isis)# net 49.0001.0001.0001.0001.00
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# redistribute isis 2 level 2
!
RP/0/RP0:hostname(config-isis-af)# interface TenGigE 0/3/0/0
RP/0/RP0:hostname(config-isis-af-if)# address-family ipv4 unicast
```

```
!
!
RP/0/RP0:hostname(config)# router isis 2
RP/0/RP0:hostname(config-isis)# is-type level-1
RP/0/RP0:hostname(config-isis)# net 49.0002.0001.0001.0002.00
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# set-attached-bit
!
RP/0/RP0:hostnamefig-isis-af)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-isis-af-if)# address-family ipv4 unicast
```

show isis

The **show isis** command displays general information about an IS-IS instance and protocol operation. If the instance ID is not specified, the command shows information about all IS-IS instances.

show isis [**instance** *instance-id*]

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS adjacencies for the specified IS-IS instance only.

Note The instance-id argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays IS-IS adjacencies for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

For each instance, the first line of output lists the IS-IS instance ID with the following lines identifying the IS-IS system ID, supported levels (level 1, level 2, or level-1-2), configured area addresses, active area addresses, status (enabled or not) and type (Cisco or IETF) of nonstop forwarding (NSF), and the mode in which the last IS-IS process startup occurred.

Next, the status of each configured address family (or just IPv4 unicast if none are configured) is summarized. For each level (level 1 or level 2), the metric style (narrow or wide) generated and accepted is listed along with the status of incremental shortest path first (iSPF) computation (enabled or not). Then redistributed protocols are listed, followed by the administrative distance applied to the redistributed routes.

Finally, the running state (active, passive, or disabled) and configuration state (active or disabled) of each IS-IS interface is listed.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis** command:

```
RP/0/RP0:hostname# show isis
Wed Aug 20 23:54:55.043 PST DST

IS-IS Router: lab
  System Id: 0000.0000.0002
  IS Levels: level-2-only
  Manual area address(es):
    49.1122
  Routing for area address(es):
    49.1122
  Non-stop forwarding: Disabled
```

```
Most recent startup mode: Cold Restart
Topologies supported by IS-IS:
  IPv4 Unicast
    Level-2
      Metric style (generate/accept): Narrow/Narrow
      Metric: 10
      ISPF status: Disabled
    No protocols redistributed
    Distance: 115
Interfaces supported by IS-IS:
  Loopback0 is running passively (passive in configuration)
  POS0/1/0/2 is running actively (active in configuration)
  POS0/1/0/3 is running actively (active in configuration
```

This table describes the significant fields shown in the display.

Table 33: show isis Field Descriptions

Field	Description
IS-IS Router	IS-IS instance ID.
System Id	IS-IS system ID.
IS Levels	Supported levels for the instance.
Manual area address(es)	Domain and area.
Routing for area address(es):	Configured area addresses and active area addresses.
Non-stop forwarding	Status (enabled or not) and type (Cisco or IETF) of nonstop forwarding (NSF).
Most recent startup mode	The mode in which the last IS-IS process startup occurred.
Topologies supported by IS-IS	The summary of the status of each configured address family (or just IPv4 unicast if none are configured).
Redistributed protocols	List of redistributed protocols, followed by the administrative distance applied to the redistributed routes.
Metric style (generate/accept)	The status of each configured address family (or just IPv4 unicast if none are configured) is summarized. For each level (level 1 or level 2), the metric style (narrow or wide) generated and accepted is listed along with the status of incremental shortest path first (iSPF) computation (enabled or not).
Interfaces supported by IS-IS	The running state (active, passive, or disabled) and configuration state (active or disabled) of each IS-IS interface.

show isis adjacency

To display Intermediate System-to-Intermediate System (IS-IS) adjacencies, use the **show isis adjacency** command.

show isis [**instance** *instance-id*] **adjacency** [**level** {**1** | **2**}] [*type interface-path-id*] [**detail**] [**systemid** *system-id*]

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS adjacencies for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
level { **1** | **2** }	(Optional) Displays the IS-IS adjacencies for Level 1 or Level 2 independently.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
detail	(Optional) Displays neighbor IP addresses and active topologies.
systemid *system-id*	(Optional) Displays the information for the specified router only.

Command Default

No instance ID specified displays IS-IS adjacencies for all the IS-IS instances.

Both Level 1 and Level 2 are configured if no level is specified.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis adjacency** command:

```
RP/0/RP0:hostname# show isis adjacency

IS-IS p Level-1 adjacencies:
System Id      Interface        SNPA           State Hold     Changed  NSF      BFD
12a4           PO0/1/0/1        *PtoP*         Up    23       00:00:06 Capable  Init
12a4           TenGigE0/6/0/2   0004.2893.f2f6 Up    56       00:04:01 Capable  Up
```

```
Total adjacency count: 2

IS-IS p Level-2 adjacencies:
System Id      Interface        SNPA           State Hold     Changed  NSF      BFD
12a4           PO0/1/0/1        *PtoP*         Up    23       00:00:06 Capable  None
12a4           TenGigE0/6/0/2   0004.2893.f2f6 Up    26       00:00:13 Capable  Init

Total adjacency count: 2
```

This table describes the significant fields shown in the display.

Table 34: show isis adjacency Field Descriptions

Field	Description
Level-1	Level 1 adjacencies.
Level-2	Level 2 adjacencies.
System ID	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or the **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
Interface	Interface used to reach the neighbor.
SNPA	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.
State	Adjacency state of the neighboring interface. Valid states are Down, Init, and Up.
Holdtime	Hold time of the neighbor.
Changed	Time the neighbor has been up (in hours:minutes:seconds).
NSF	Specifies whether the neighbor can adhere to the IETF-NSF restart mechanism.
BFD	Specifies the Bidirectional Forwarding Detection (BFD) status for the interface. Valid status are: • None—BFD is not configured. • Init—BFD session is not up. One reason is that other side is not yet enabled. • Up—BFD session has been established. • Down—BFD session holdtime expired.

show isis adjacency-log

To display the Intermediate System-to-Intermediate System (IS-IS) adjacency log, use the **show isis adjacency-log** command.

show isis adjacency-log [**level** {**1** | **2**}] [{**last** *number* | **first** *number*}]

Syntax Description

level { **1** | **2** }	(Optional) Displays the IS-IS adjacency log for Level 1 or Level 2 independently.
last *number*	(Optional) Specifies that the output is restricted to the last *number* of entries. Range is 1 to 100.
first *number*	(Optional) Specifies that the output is restricted to the first *number* of entries. Range is 1 to 100.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis adjacency-log** command:

```
RP/0/RP0:hostname# show isis adjacency-log

   IS-IS 10 Level 1 Adjacency log
When           System          Interface          State   Details
4d00h          12a1            PO0/5/0/0          d -> i
4d00h          12a1            PO0/5/0/0          i -> u  New adjacency
                                                          IPv4 Unicast Up
4d00h          12a1            TenGigE0/6/0/0     d -> u  New adjacency
4d00h          12a1            TenGigE0/6/0/0     u -> d  Interface state
down
3d17h          12a1            TenGigE0/6/0/0     d -> u  New adjacency
3d17h          12a1            TenGigE0/6/0/0     u -> d  Interface state
down
01:44:07       12a1            TenGigE0/6/0/0     d -> u  New adjacency

   IS-IS 10 Level 2 Adjacency log
When           System          Interface          State   Details
4d00h          12a1            PO0/5/0/0          d -> i
4d00h          12a1            PO0/5/0/0          i -> u  New adjacency
                                                          IPv4 Unicast Up
4d00h          12a1            TenGigE0/6/0/0     d -> u  New adjacency
4d00h          12a1            TenGigE0/6/0/0     u -> d  Interface state
down
```

```
3d17h          12a1            TenGigE0/6/0/0     d -> u  New adjacency
3d17h          12a1            TenGigE0/6/0/0     u -> d  Interface state
down
01:44:07       12a1            TenGigE0/6/0/0     d -> u  New adjacency
```

This table describes the significant fields shown in the display.

Table 35: show isis adjacency-log Field Descriptions

Field	Description
When	Elapsed time (in hh:mm:ss) since the event was logged.
System	System ID of the adjacent router.
Interface	Specific interface involved in the adjacency change.
State	State transition for the logged event.
Details	Description of the adjacency change.

show isis checkpoint adjacency

To display the Intermediate System-to-Intermediate System (IS-IS) checkpoint adjacency database, use the **show isis checkpoint adjacency** command.

show isis [**instance** *instance-id*] **checkpoint adjacency**

Syntax Description

instance	*instance-id*	(Optional) Displays the IS-IS checkpoint adjacencies for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays IS-IS checkpoint adjacencies for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show isis checkpoint adjacency** command to display the checkpointed adjacencies. With this information you can restore the adjacency database during a Cisco proprietary nonstop forwarding (NSF) restart. This command, with the **show isis adjacency** command, can be used to verify the consistency of the two databases.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis checkpoint adjacency** command:

```
RP/0/RP0:hostname# show
          isis
          checkpoint
          adjacency

 Interface        Level  System ID        State  Circuit ID          Chkpt ID
 TenGigE3/0/0/1     1    router-gsr8       Up     0001.0000.0008.04   80011fec
 TenGigE0/4/0/1     1    router-gsr9       Up     0001.0000.0006.01   80011fd8
 TenGigE/0/0/1      2    router-gsr8       Up     0001.0000.0008.04   80011fc4
```

This table describes the significant fields shown in the display.

Table 36: show isis checkpoint adjacency Field Descriptions

Field	Description
Interface	Interface used to reach the neighbor.
Level	Lists either routers with Level 1 or Level 2 adjacency configured.
System ID	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
State	State of the neighboring interface.
Circuit ID	Unique ID issued to a circuit at its creation.
Chkpt ID	Unique ID issued to the checkpoint at its creation.

show isis checkpoint interface

To display the Intermediate System-to-Intermediate System (IS-IS) checkpoint interfaces, use the **show isis checkpoint interface** command.

show isis checkpoint interface

This command has no keywords or arguments.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis checkpoint interface** command:

```
RP/0/RP0:hostname# show isis checkpoint interface

IS-IS 10 checkpoint interface
Interface         Index  CircNum  DIS Areas    Chkpt ID
PO0/5/0/0         0      0        NONE         80002fe8
TenGigE0/6/0/0    1      3        L1L2         80002fd0
```

This table describes the significant fields shown in the display.

Table 37: show isis checkpoint interface Field Descriptions

Field	Description
Interface	Interface used to reach the neighbor.
Index	Interface index assigned to an interface upon its creation.
CircNum	Unique ID issued to a circuit internally.
DIS Areas	Designated Intermediate System area.
Chkpt ID	Unique ID issued to the checkpoint at its creation.

show isis checkpoint lsp

To display the Intermediate System-to-Intermediate System (IS-IS) checkpoint link-state packet (LSP) protocol data unit (PDU) identifier database, use the **show isis checkpoint lsp** command.

show isis [**instance** *instance-id*] **checkpoint lsp**

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS checkpoint LSPs for the specified instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays IS-IS checkpoint LSPs for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The checkpointed LSPs displayed by this command are used to restore the LSP database during a Cisco-proprietary nonstop forwarding (NSF) restart. The **show isis checkpoint lsp** command, with the **show isis database** command, may be used to verify the consistency of the two databases.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis checkpoint lsp** command:

```
RP/0/RP0:hostname# show isis checkpoint lsp

Level  LSPID              Chkpt ID
1      router-gsr6.00-00  80011f9c
1      router-gsr6.01-00  80011f88
1      router-gsr8.00-00  80011f74
1      router-gsr9.00-00  80011f60
2      router-gsr6.00-00  80011f4c
2      router-gsr6.01-00  80011f38
2      router-gsr8.00-00  80011f24
2      router-gsr9.00-00  80011f10
Total LSP count: 8 (L1: 4, L2 4, local L1: 2, local L2 2)
```

This table describes the significant fields shown in the display.

Table 38: show isis checkpoint lsp Field Descriptions

Field	Description
Level	Routers with Level 1 or Level 2 adjacency configured.
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
Chkpt ID	Unique ID issued to the checkpoint at its creation.

show isis database

To display the Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) database, use the **show isis database** command.

show isis [**instance** *instance-id*] **database** [**level** {**1** | **2**}] [**update**] [**summary**] [**detail**] [**verbose**] [{***lsp-id***}]

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS LSP database for the specified instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
level { **1** | **2** }	(Optional) Displays the IS-IS LSP database for Level 1 or Level 2 independently.
update	(Optional) Displays contents of LSP database managed by update thread.
summary	(Optional) Displays the LSP ID number, sequence number, checksum, hold time, and bit information.
detail	(Optional) Displays the contents of each LSP.
verbose	(Optional) Displays the contents of each LSP.
* | *lsp-id*	(Optional) LSP protocol data units (PDUs) identifier. Displays the contents of a single LSP by its ID number or may contain an * as a wildcard character.

Command Default

No instance ID specified displays the IS-IS LSP database for all the IS-IS instances.

Both Level 1 and Level 2 is configured if no level is specified.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Each of the options for the **show isis database** command can be entered in an arbitrary string within the same command entry. For example, the following are both valid command specifications and provide the same output: **show isis database detail level 2** and **show isis database level 2 detail** .

The **summary** keyword used with this command allows you to filter through a large IS-IS database and quickly identify problematic areas.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis database** command with the **summary** keyword:

```
RP/0/RP0:hostname# show isis database summary

  IS-IS 10 Database Summary for all LSPs
                                Active              Purged               All
                           L1    L2   Total    L1    L2   Total    L1    L2   Total
                          ----- ----- -----  ----- ----- -----  ----- ----- -----
  Fragment 0 Counts
              Router LSPs:     1     1     2      0     0     0      1     1     2
        Pseudo-node LSPs:     0     0     0      0     0     0      0     0     0
                 All LSPs:     1     1     2      0     0     0      1     1     2
  Per Topology
      IPv4 Unicast
        ATT bit set LSPs:     0     0     0      0     0     0      0     0     0
        OVL bit set LSPs:     0     0     0      0     0     0      0     0     0

  All Fragment Counts
              Router LSPs:     1     1     2      0     0     0      1     1     2
        Pseudo-node LSPs:     0     0     0      0     0     0      0     0     0
                 All LSPs:     1     1     2      0     0     0      1     1     2
```

This table describes the significant fields shown in the display.

Table 39: show isis database summary Field Descriptions

Field	Description
Router LSPs	Active, purged, and total LSPs associated with routers.
Pseudo-node LSPs:	Active, purged, and total LSPs associated with pseudonodes.
All LSPs:	Total active and purged LSPs.
ATT bit set LSPs	Attach bit (ATT). Indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point to a default route to the closest Level 2 router.
OVL bit set LSPs	Overload bit. Indicates if the IS is congested. If the Overload bit is set, other routers do not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router are sent to this router.

show isis database-log

To display the entries in the Intermediate System-to-Intermediate System (IS-IS) database log, use the **show isis database-log** command.

show isis database-log [**level** {**1** | **2**}] [{**last** *number* | **first** *number*}]

Syntax Description

level { **1** | **2** }	(Optional) Displays the database log for Level 1 or Level 2 independently.
last *number*	(Optional) Specifies that the output be restricted to the last *number* of entries. Range is 1 to 1000.
first *number*	(Optional) Specifies that the output be restricted to the first *number* of entries. Range is 1 to 1000.

Command Default

Both Level 1 and Level 2 are configured if no level is specified.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis database-log** command:

```
RP/0/RP0:hostname# show isis database-log

   IS-IS 10 Level 1 Link State Database Log
                                  New LSP                  Old LSP
WHEN     LSPID                 Op  Seq Num    Holdtime OL  Seq Num    Holdtime OL
01:17:19 12b1.03-00            REP 0x00000003 1200      0  0x00000002 340       0
001:06:20 12b1.00-00           REP 0x000001d8 1200      0  0x000001d7 375       0
01:06:00 12b1.03-00            REP 0x00000004 1200      0  0x00000003 520       0
01:05:46 12a1.00-00            REP 0x000001fc 1200      0  0x000001fb 425       0
00:55:01 12b1.00-00            REP 0x000001d9 1200      0  0x000001d8 520       0
00:53:39 12b1.03-00            REP 0x00000005 1200      0  0x00000004 459       0
00:53:19 12a1.00-00            REP 0x000001fd 1200      0  0x000001fc 453       0
00:42:12 12b1.00-00            REP 0x000001da 1200      0  0x000001d9 431       0
00:39:56 12b1.03-00            REP 0x00000006 1200      0  0x00000005 376       0
00:38:54 12a1.00-00            REP 0x000001fe 1200      0  0x000001fd 334       0
00:29:10 12b1.00-00            REP 0x000001db 1200      0  0x000001da 418       0
00:27:22 12b1.03-00            REP 0x00000007 1200      0  0x00000006 446       0
00:25:10 12a1.00-00            REP 0x000001ff 1200      0  0x000001fe 375       0
00:17:04 12b1.00-00            REP 0x000001dc 1200      0  0x000001db 473
```

This table describes the significant fields shown in the display.

Table 40: show isis database-log Field Descriptions

Field	Description
WHEN	Elapsed time (in hh:mm:ss) since the event was logged.
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is 0, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
New LSP	New router or pseudonode appearing in the topology.
Old LSP	Old router or pseudonode leaving the topology.
Op	Operation on the database: inserted (INS) or replaced (REP).
Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
Holdtime	Time the LSP remains valid (in seconds). An LSP hold time of 0 indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP stays in the LSDB before being completely removed.
OL	Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers do not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router are sent to this router.

show isis fast-reroute

To display per-prefix LFA information, use the **show isis fast-reroute** command.

show isis fast-reroute
A.B.C.D/length | **detail** | **summary**

Syntax Description

A.B.C.D/length	Network to show per-prefix LFA information.
detail	Use to display tiebreaker information about the backup.
summary	Use to display the number of prefixes having protection per priority.

Command Default

None

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

The following is sample output from **show isis fast-reroute** command that displays per-prefix LFA information:

```
RP/0/RP0:hostname# show isis fast-reroute 10.1.6.0/24

L1 10.1.6.0/24 [20/115]
     via 10.3.7.47, POS0/3/0/1, router2
       FRR backup via 10.1.7.145, TenGigE0/1/0/3, router3
```

The following is sample output from **show isis fast-reroute detail** command that displays tie-breaker information about the backup:

```
RP/0/RP0:hostname# show isis fast-reroute 10.1.6.0/24 detail

L1 10.1.6.0/24 [20/115] low priority
     via 10.3.7.47, POS0/3/0/1, router2
       FRR backup via 10.1.7.145, TenGigE0/1/0/3, router3
       P: No, TM: 30, LC: Yes, NP: No, D: No
     src router2.00-00, 192.168.0.47
   L2 adv [20] native, propagated
```

The following is sample output from **show isis fast-reroute summary** command that displays the number of prefixes having protection per priority:

```
RP/0/RP0:hostname#show isis fast-reroute summary
IS-IS frr IPv4 Unicast FRR summary
```

```
                                  Critical   High       Medium     Low        Total
                                  Priority   Priority   Priority   Priority
Prefixes reachable in L1
  All paths protected     0           0          2          8          10
  Some paths protected 0              0          1          3          4
  Unprotected               0         0          1          3
 4
  Protection coverage    0.00%     0.00%     75.00%     78.57%     77.78%
Prefixes reachable in L2
  All paths protected     0           0          0          0          0
  Some paths protected 0              0          1          0          1
  Unprotected               0         0          0          0
 0
  Protection coverage    0.00%     0.00%     100.00%    0.00%      100.00%
```

show isis hostname

To display the entries in the Intermediate System-to-Intermediate System (IS-IS) router name-to-system ID mapping table, use the **show isis hostname** command.

show isis [**instance** *instance-id*] **hostname**

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS router name-to-system ID mapping table for the specified IS-IS instance only. The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays the IS-IS router name-to-system ID mapping table for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **show isis hostname** command does not display entries if the dynamic hostnames are disabled.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis hostname** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0:hostname# show isis instance isp hostname

ISIS isp hostnames
    Level  System ID      Dynamic Hostname
     1     0001.0000.0005 router
     2   * 0001.0000.0011 router-11
```

This table describes the significant fields shown in the display.

Table 41: show isis instance isp hostname Field Descriptions

Field	Description
Level	IS-IS level of the router.
System ID	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or **hostname dynamic disable** command has been executed, the 6-octet system ID is used.

Field	Description
Dynamic Hostname	Hostname of the router.
*	Local router.

show isis interface

To display information about the Intermediate System-to-Intermediate System (IS-IS) interfaces, use the **show isis interface** command.

show isis interface [{*type interface-path-id* | **level** {**1** | **2**}}] [**brief**]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
level { **1** | **2** }	(Optional) Displays IS-IS interface information for Level 1 or Level 2 independently.
brief	(Optional) Displays brief interface output.

Command Default

Displays all IS-IS interfaces.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis interface** command:

```
RP/0/RP0:hostname#show isis interface
          TenGigE interface 0/3/0/2
 TenGigE 0/3/0/2                 Enabled
  Adjacency Formation:       Enabled
  Prefix Advertisement:      Enabled
  BFD:                       Disabled
  BFD Min Interval:          150
  BFD Multiplier:            3

  Circuit Type:              level-2-only
  Media Type:                P2P
  Circuit Number:            0
  Extended Circuit Number:   67111168
  Next P2P IIH in:           4 s
  LSP Rexmit Queue Size:     0
```

```
Level-2
  Adjacency Count:        1
  LSP Pacing Interval:    33 ms
  PSNP Entry Queue Size:  0

CLNS I/O
  Protocol State:         Up
  MTU:                    4469

IPv4 Unicast Topology:    Enabled
  Adjacency Formation:    Running
  Prefix Advertisement:   Running
  Metric (L1/L2):         10/100
  MPLS LDP Sync (L1/L2):  Disabled/Disabled


IPv4 Address Family:      Enabled
  Protocol State:         Up
  Forwarding Address(es): 10.3.10.143
  Global Prefix(es):      10.3.10.0/24


LSP transmit timer expires in 0 ms
LSP transmission is idle
Can send up to 9 back-to-back LSPs in the next 0 ms
```

This table describes the significant fields shown in the display.

Table 42: show isis interface Field Descriptions

Field	Description
TenGigE0/6/0/0	Status of the interface, either enabled or disabled.
Adjacency formation	Status of adjacency formation, either enabled or disabled.
Prefix Advertisement	Status of advertising connected prefixes, either enabled or disabled.
BFD	Status of Bidirectional Forwarding Detection (BFD), either enabled or disabled.
BFD Min Interval	BFD minimum interval.
BFD Multiplier	BFD multiplier.
Circuit Type	Levels the interface is running on (circuit-type configuration) which may be a subset of levels on the router.
Media Type	Media type on which IS-IS is running.
Circuit Number	Unique ID assigned to a circuit internally (8-bit integer).
Extended Circuit Number	Valid only for point-to-point interfaces (32-bit integer).
LSP Rexmit Queue Size	Number of LSPs pending retransmission on the interface.
Adjacency Count	Number of adjacencies formed with a neighboring router that supports the same set of protocols.

Field	Description
PSNP Entry Queue Size	Number of SNP entries pending inclusion in the next PSNP.
LAN ID	ID of the LAN.
Priority (Local/DIS)	Priority of this interface or priority of the Designated Intermediate System.
Next LAN IIH in	Time (in seconds) in which the next LAN hello message is sent.
LSP Pacing Interval	Interval at which the link-state packet (LSP) transmission rate (and by implication the reception rate of other systems) is to be reduced.
Protocol State	Running state of the protocol (up or down).
MTU	Link maximum transmission unit (MTU).
SNPA	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.
IPv4 Unicast Topology	Status of the topology, either enabled or disabled.
Adjacency Formation	Status of adjacency formation. The status options are Running or a reason for not being ready to form adjacencies.
Prefix Advertisement	Status of advertising prefixes, either enabled or disabled.
Metric (L1/L2)	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a connectionless network service (CLNS) prefix).
MPLS LDP Sync (L1/L2)	Status of LDP IS-IS synchronization, either enabled or disabled. When enabled, the state of synchronization (Sync Status) is additionally displayed as either achieved or not achieved.
IPv4 Address Family	Status of the address family, either enabled or disabled.
Protocol State	State of the protocol.
Forwarding Address(es)	Addresses on this interface used by the neighbor for next-hop forwarding.
Global Prefix(es)	Prefixes for this interface included in the LSP.
LSP transmit timer expires in	LSP transmission expiration timer interval (in milliseconds).
LSP transmission is	State of LSP transmission. Valid states are • idle • in progress • requested • requested and in progress

The following is sample output from the **show isis interface** command with the **brief** keyword:

```
RP/0/RP0:hostname# show isis interface brief

    Interface      All     Adjs    Adj Topos  Adv Topos  CLNS   MTU    Prio
                   OK    L1   L2    Run/Cfg    Run/Cfg                L1   L2
-----------------  ---  ---------  ---------  ---------  ----  ----  --------
PO0/5/0/0          Yes    1    1       1/1        1/1     Up    4469    -    -
TenGigE0/6/0/0     Yes    1*   1*      1/1        1/1     Up    1497   64   64
```

This table describes the significant fields shown in the display.

Table 43: show isis interface brief Field Descriptions

Field	Description
Interface	Name of the interface.
All OK	Everything is working as expected for this interface.
Adjs L1 L2	Number of L1 and L2 adjacencies over this interface.
Adj Topos Run/Cfg	Number of topologies that participate in forming adjacencies. Number of topologies that were configured to participate in forming adjacencies.
Adv Topos Run/Cfg	Number of topologies that participate in advertising prefixes. Number of topologies that were configured to participate in advertising prefixes.
CLNS	Status of the Connectionless Network Service. Status options are Up or Down.
MTU	Maximum transfer unit size for the interface.
Prio L1 L2	Interface L1 priority. Interface L2 priority.

show isis lsp-log

To display link-state packet (LSP) log information, use the **show isis lsp-log** command.

show isis [**instance** *instance-id*] **lsp-log** [**level** {**1** | **2**}] [{**last** *number* | **first** *number*}]

Syntax Description

instance *instance-id*	(Optional) Displays the LSP log information for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
level { **1** | **2** }	(Optional) Displays the Intermediate System-to-Intermediate System (IS-IS) link-state database for Level 1 or Level 2 independently.
last *number*	(Optional) Specifies that the output be restricted to the last *number* of entries. Range is 1 to 20.
first *number*	(Optional) Specifies that the output be restricted to the first *number* of entries. Range is 1 to 20.

Command Default

No instance ID specified displays the LSP log information for all the IS-IS instances.

Both Level 1 and Level 2 are configured if no level is specified.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis lsp-log** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0:hostname# show isis instance isp lsp-log

ISIS isp Level 1 LSP log
  When       Count      Interface       Triggers
00:02:36         1
00:02:31         1                      LSPREGEN
00:02:26         1      PO4/1           DELADJ
00:02:24         1      PO4/1           NEWADJ
00:02:23         1      TenGigE5/0      DIS
00:01:27         1      Lo0             IPDOWN
00:01:12         1      Lo0             IPUP


ISIS isp Level 2 LSP log
  When       Count      Interface       Triggers
```

```
00:02:36         1
00:02:30         1                        LSPREGEN
00:02:26         1       PO4/1            DELADJ
00:02:24         1       PO4/1            NEWADJ
00:02:23         1       TenGigE5/0       DIS
00:02:21         1                        AREASET
00:01:27         1       Lo0              IPDOWN
00:01:12         1       Lo0              IPUP
```

This table describes the significant fields shown in the display.

Table 44: show isis instance isp lsp-log Field Descriptions

Field	Description
Level	IS-IS level of the router.
When	How long ago (in hh:mm:ss) an LSP rebuild occurred. The last 20 occurrences are logged.
Count	Number of events that triggered this LSP run. When there is a topology change, often multiple LSPs are received in a short period. A router waits 5 seconds before running a full LSP, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting its 5 seconds before running full LSP.
Interface	Interface that corresponds to the triggered reasons for the LSP rebuild.
Triggers	A list of all reasons that triggered an LSP rebuild. The triggers are • AREASET—area set changed • ATTACHFLAG—bit attached • CLEAR— **clear** command • CONFIG—configuration change • DELADJ—adjacency deleted • DIS—DIS changed • IFDOWN—interface down • IPADDRCHG—IP address change • IPDEFORIG—IP def-orig • IPDOWN—connected IP down • IFDOWN—interface down • IPEXT—external IP • IPIA—nterarea IP • IPUP—connected IP up • LSPDBOL—LSPDBOL bit • LSPREGEN—LSP regeneration • NEWADJ— new adjacency

show isis mesh-group

To display Intermediate System-to-Intermediate System (IS-IS) mesh group information, use the **show isis mesh-group** command.

show isis [**instance** *instance-id*] **mesh-group**

Syntax Description

instance	*instance-id*	(Optional) Displays the mesh group information for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays the IS-IS mesh group information for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis mesh-group** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0:hostname# show isis instance isp mesh-group

 ISIS isp Mesh Groups

 Mesh group 6:
 TenGigE 0/4/0/1
```

This table describes the significant fields shown in the display.

Table 45: show isis instance isp mesh-group Field Descriptions

Field	Description
Mesh group	Mesh group number to which this interface is a member. A mesh group optimizes link-state packet (LSP) flooding in nonbroadcast multiaccess (NBMA) networks with highly meshed, point-to-point topologies. LSPs that are first received on interfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group.
TenGigE0/4/0/1	Interface belonging to mesh group 6.

show isis mpls traffic-eng adjacency-log

To display a log of Multiprotocol Label Switching traffic engineering (MPLS TE) adjacency changes for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis mpls traffic-eng adjacency-log** command.

show isis [**instance** *instance-id*] **mpls traffic-eng adjacency-log** [{**last** *number* | **first** *number*}]

Syntax Description

instance *instance-id*	(Optional) Displays the MPLS TE adjacency changes for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
last *number*	(Optional) Specifies that the output is restricted to last *number* of entries. Range is 1 to 20.
first *number*	(Optional) Specifies that the output is restricted to first *number* of entries. Range is 1 to 20.

Command Default

No instance ID specified displays MPLS TE adjacency changes for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show isis mpls traffic-eng adjacency-log** command to display the status of MPLS TE adjacencies.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis mpls traffic-eng adjacency-log** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0:hostname# show isis instance isp mpls traffic-eng adjacency-log

IS-IS isp Level-2 MPLS Traffic Engineering adjacency log
When      Neighbor ID        IP Address       Interface Status
00:03:36  router-6           172.17.1.6         PO0/3/0/1 Up
00:03:36  router-6           172.17.1.6         PO0/3/0/1 Down
00:02:38  router-6           172.17.1.6         PO0/3/0/1 Up
```

This table describes the significant fields shown in the display.

Table 46: show isis instance isp mpls traffic-eng adjacency-log Field Descriptions

Field	Description
When	Time (in hh:mm:ss) since the entry was recorded in the log.
Neighbor ID	Identification value of the neighbor.
IP Address	Neighbor IP Version 4 (IPv4) address.
Interface	Interface from which a neighbor is learned.
Status	Up (active) or Down (disconnected).

show isis mpls traffic-eng advertisements

To display the latest flooded record from Multiprotocol Label Switching traffic engineering (MPLS TE) for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis mpls traffic-eng advertisements** command.

show isis [**instance** *instance-id*] **mpls traffic-eng advertisements**

Syntax Description

instance *instance-id*	(Optional) Displays the latest flooded record from MPLS TE for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays the latest flooded record from MPLS TE for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show isis mpls traffic-eng advertisements** command to verify that MPLS TE is flooding its record and that the bandwidths are correct.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis mpls traffic-eng advertisements** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0:hostname# show isis instance isp mpls traffic-eng advertisements

 ISIS isp Level-2 MPLS Traffic Engineering advertisements
       System ID: router-9
       Router ID: 172.18.0.9
       Link Count: 1
         Link[0]
           Neighbor System ID: router-gsr6 (P2P link)
           Interface IP address: 172.18.0.9
           Neighbor IP Address: 172.18.0.6
           Admin. Weight: 0
           Physical BW: 155520000 bits/sec
           Reservable BW global: 10000000 bits/sec
           Reservable BW sub: 0 bits/sec
           Global pool BW unreserved:
             [0]: 10000000 bits/sec, [1]: 10000000 bits/sec
             [2]: 10000000 bits/sec, [3]: 10000000 bits/sec
             [4]: 10000000 bits/sec, [5]: 10000000 bits/sec
             [6]: 10000000 bits/sec, [7]: 10000000 bits/sec
```

```
Sub pool BW unreserved:
  [0]: 0 bits/sec, [1]: 0 bits/sec
  [2]: 0 bits/sec, [3]: 0 bits/sec
  [4]: 0 bits/sec, [5]: 0 bits/sec
  [6]: 0 bits/sec, [7]: 0 bits/sec
Affinity Bits: 0x00000000
```

This table describes the significant fields shown in the display.

Table 47: show isis instance isp mpls traffic-eng advertisements Field Descriptions

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or if the **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
Router ID	MPLS TE router ID.
Link Count	Number of links that MPLS TE advertised.
Neighbor System ID	System ID of a neighbor number in an area. The six bytes directly preceding the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2). In an IS-IS routing domain, each router is represented by a 6-byte hexadecimal system ID. When network administrators maintain and troubleshoot networking devices, they must know the router name and corresponding system ID.
Interface IP address	IP address of the interface.
Neighbor IP Address	IP address of the neighbor.
Admin. Weight	Administrative weight associated with this link.
Physical BW	Link bandwidth capacity (in bits per second).
Reservable BW	Reservable bandwidth on this link.
Global pool BW unreserved	Unreserved bandwidth that is available in the global pool.
Sub pool BW unreserved	Amount of unreserved bandwidth that is available in the subpool.
Affinity Bits	Link attribute flags being flooded. Bits are MPLS-TE specific.

show isis mpls traffic-eng tunnel

To display Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel information for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis mpls traffic-eng tunnel** command.

show isis [**instance** *instance-id*] **mpls traffic-eng tunnel**

Syntax Description

instance	*instance-id*	(Optional) Displays the MPLS TE tunnel information for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays the MPLS TE tunnel information for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show isis** command to find the current status of MPLS TE tunnels.

Tunnels are used in IS-IS next-hop calculations.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis mpls traffic-eng tunnel** command:

```
RP/0/RP0:hostname# show isis mpls traffic-eng tunnel

ISIS isp Level-2 MPLS Traffic Engineering tunnels
    System Id           Tunnel Name   Bandwidth    Nexthop       Metric   Mode
    router-6            tu0           100000       172.18.1.6      0        Relative
```

This table describes the significant fields shown in the display.

Table 48: show isis mpls traffic-eng tunnel Field Descriptions

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
Tunnel Name	Name of the MPLS TE tunnel interface.

Field	Description
Bandwidth	MPLS TE-specified tunnel bandwidth of the tunnel.
Nexthop	MPLS TE destination IP address of the tunnel.
Metric	MPLS TE metric of the tunnel.
Mode	MPLS TE metric mode of the tunnel. It can be relative or absolute.

show isis neighbors

To display information about Intermediate System-to-Intermediate System (IS-IS) neighbors, use the **show isis neighbors** command.

show isis [**instance** *instance-id*] **neighbors** [{*type interface-path-id* | **summary**}] [**detail**] [**systemid** *system-id*]

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS neighbor information for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
summary	(Optional) Displays neighbor status count for each level.
detail	(Optional) Displays additional details.
systemid *system-id*	(Optional) Displays the information for the specified neighbor only.

Command Default

No instance ID specified displays neighbor information for all the IS-IS instances.

Both Level 1 and Level 2 are configured if no level is specified.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis neighbors** command with the **instance** and *instance-id* values specified:

```
Total neighbor count: 3
RP/0/RP0:hostname# show isis instance isp neighbors detail
```

```
IS-IS isp neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
e222e          TenGigE0/1/0/0   *PtoP*         Up    23       L1   Capable
  Area Address(es): 00
  IPv4 Address(es): 10.1.0.45*
  Topologies: 'IPv4 Unicast'
  Uptime: 01:09:44
  IPFRR: LFA Neighbor: elise
         LFA IPv4 address: 10.100.1.2
         LFA Router address: 192.168.0.45
TenGigE0/1/0/0.
e333e          TenGigE0/1/0/0.1 0012.da6b.68a8 Up    8        L1   Capable
  Area Address(es): 00
  IPv4 Address(es): 10.100.1.2*
  Topologies: 'IPv4 Unicast'
  Uptime: 01:09:46
  IPFRR: LFA Neighbor: elise
         LFA IPv4 address: 10.1.0.45
         LFA Router address: 192.168.0.45
         LFA Interface: TenGigE0/1/0/0
m44i           TenGigE0/1/0/1   0012.da62.e0a8 Up    7        L1   Capable
  Area Address(es): 00 11
  IPv4 Address(es): 10.1.2.47*
  Topologies: 'IPv4 Unicast'
  Uptime: 01:09:33

Total neighbor count: 3
```

This table describes the significant fields shown in the display.

Table 49: show isis instance isp neighbors Field Descriptions

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
Interface	Interface through which the neighbor is reachable.
SNPA	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.
State	Adjacency state of the neighboring interface. Valid states are: Down, Init, and Up.
Holdtime	Hold time of the neighbor.
Type	Type of adjacency.
IETF-NSF	Specifies whether the neighbor can adhere to the IETF-NSF restart mechanism. Valid states are Capable and Unable.
Area Address(es)	Number of area addresses on this router.
IPv4 Address(es)	IPv4 addresses configured on this router.
Topologies	Address and subaddress families for which IS-IS is configured.

Field	Description
Uptime	Time (in hh:mm:ss) that the neighbor has been up.
IPFRR: LFA Neighbor	IP fast reroute (IPFRR) loop-free alternate (LFA) neighbor.
LFA IPv4 address:	Address of the LFA.
LFA Interface:	LFA interface.

The following is sample output from the **show isis neighbors** command with the **summary** keyword specified:

```
RP/0/RP0:hostname# show isis instance isp neighbors summary

ISIS isp neighbor summary:
    State          L1       L2     L1L2
    Up              0        0        2
    Init            0        0        0
    Failed          0        0        0
```

This table describes the significant fields shown in the display.

Table 50: show isis neighbors summary Field Descriptions

Field	Description
State	State of the neighbor is up, initialized, or failed.
L1	Number of Level 1 neighbors.
L2	Number of Level 2 neighbors.
LlL2	Number of Level 1 and 2 neighbors.

show isis protocol

To display summary information about an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis protocol** command.

show isis [**instance** *instance-id*] **protocol**

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS adjacencies for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays IS-IS adjacencies for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis protocol** command:

```
RP/0/RP0:hostname# show isis protocol

IS-IS Router: isp
      System Id: 0001.0000.0011
      IS Levels: level-1-2
      Manual area address(es):
        49

      Routing for area address(es):
        49
      Non-stop forwarding: Cisco Proprietary NSF Restart enabled
      Process startup mode: Cold Restart
      Topologies supported by IS-IS:
        IPv4 Unicast
          Level-1 iSPF status: Dormant (awaiting initial convergence)
          Level-2 iSPF status: Dormant (awaiting initial convergence)
          No protocols redistributed
          Distance: 115
      Interfaces supported by IS-IS:
        Loopback0 is running passively (passive in configuration)
        TenGigE 0/4/0/1 is running actively (active in configuration)
        TenGigE 0/5/0/1 is running actively (active in configuration)
```

This table describes the significant fields shown in the display.

Table 51: show isis protocol Field Descriptions

Field	Description
System ID:	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
IS Levels:	IS-IS level of the router.
Manual area address(es)	Area addresses that are manually configured.
Routing for areaaddress(es)	Area addresses for which this router provides the routing.
Non-stop forwarding:	Status and name of nonstop forwarding (NSF).
Process startup mode:	Mode in which the last process startup occurred. Valid modes are: • Cisco Proprietary NSF Restart • IETF NSF Restart • Cold Restart
iSPF status:	State of incremental shortest path first (iSPF) configuration for this IS-IS instance. Four states exist: Disabled if iSPF has not been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. Dormant if iSPF has been configured but is awaiting initial convergence before initializing. Awake if iSPF has been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. Active if IS-IS is ready to consider using the iSPF algorithm whenever a new route calculation needs to be run.
No protocols redistributed:	No redistributed protocol information exists to be displayed.
Distance:	Administrative distance for this protocol.

show isis route

To display IP reachability information for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis route** command.

show isis [**instance** *instance-id*] [{**ipv4** | **afi-all**}] [{**unicast** | [**topology** {**all***topo-name*}] | **safi-all**}] **route** [{*ip-address mask* | *ip-address*/*length* [**longer-prefixes**]}] [**summary**] [**backup**] [**detail**]

Syntax Description

instance *instance-id*	(Optional) Displays the IP reachability information for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
afi-all	(Optional) Specifies all address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
topology	(Optional) Specifies IS-IS paths to intermediate systems.
all	(Optional) Specifies all topologies.
topology *topo-name*	(Optional) Specifies topology table information and name of the topology table.
safi-all	(Optional) Specifies all secondary address prefixes.
ip-address	(Optional) Network IP address about which routing information should be displayed.
mask	(Optional) Network mask specified in either of two ways: • Network mask can be a four-part, dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. • Network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are the network address.
/ *length*	(Optional) Length of the IP prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value. Range is 0 to 32.
longer-prefixes	(Optional) Displays route and more-specific routes.
summary	(Optional) Displays topology summary information.
systemid	(Optional) Displays multicast information by system ID.
backup	(Optional) Displays backup information for this entry.
detail	(Optional) Displays link-state packet (LSP) details.

Command Default No instance ID specified displays the IP reachability information for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples The following is sample output from the **show isis route** command:

```
RP/0/RP0:hostname# show isis route

IS-IS isp IPv4 Unicast routes
Codes: L1 - level 1, L2 - level 2, ia - interarea (leaked into level 1)
df - level 1 default (closest attached router), su - summary null
C - connected, S - static, R - RIP, B - BGP, O - OSPF
i - IS-IS (redistributed from another instance)

Maximum parallel path count: 8

L2 10.76.240.6/32 [4/115]
via 10.76.245.252, SRP0/1/0/2, isp2
via 10.76.246.252, SRP0/1/0/0, isp2
C 10.76.240.7/32
is directly connected, Loopback0
L2 10.76.240.9/32 [256/115]
via 10.76.249.2, TenGigE 0/3/0/0, isp3
L2 10.76.240.10/32 [296/115]
via 10.76.249.2, TenGigE 0/3/0/0, isp3
C 10.76.245.0/24
is directly connected, SRP0/1/0/2
C 10.76.246.0/24
is directly connected, SRP0/1/0/0
C 10.76.249.0/26
is directly connected, TenGigE 0/3/0/0
L2 10.101.10.0/24 [296/115]
via 10.76.249.2, TenGigE 0/3/0/0, isp3
```

This table describes the significant fields shown in the display.

Table 52: show isis route ipv4 unicast Field Descriptions

Field	Description
C172.18.0.0/24	Connected route for TenGigabit Ethernet interface 0/5/0/0.
C 172.19.1.0/24	Connected route for TenGigabit Ethernet interface 0/4/0/1.
L1 172.35.0.0/24 [10]	Level 1 route to network 172.35.0.0/24.
C 172.18.0/24	Connected route for loopback interface 0.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command.

show isis [**instance** *instance-id*] [[{**ipv4** | **afi-all**}] [{**unicast** | [**topology** {**all***topo-name*}] | **safi-all**}]] **spf-log** [**level** {**1** | **2**}] [{**ispf** | **fspf** | **prc** | **nhc**}] [{**detail** | **verbose** | **plfrr** | **ppfrr**}] [{**last** *number* | **first** *number*}]

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS SPF log for the specified IS-IS instance only.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
afi-all	(Optional) Specifies all address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
topology all | *topo-name*	(Optional) Specifies topology table information for all topologies or for the specified topology table (*top-name*).
safi-all	(Optional) Specifies all secondary address prefixes.
level { **1** | **2** }	(Optional) Displays the IS-IS SPF log for Level 1 or Level 2 independently.
ispf	(Optional) Specifies incremental SPF entries only.
fspf	(Optional) Specifies full SPF entries only.
prc	(Optional) Specifies partial route calculations only.
nhc	(Optional) Specifies next-hop route calculations only.
detail	(Optional) Specifies detailed output. Includes a breakdown of the time taken to perform the calculation and changes resulting from the calculation.
verbose	(Optional) Specifies verbose output.
last *number*	(Optional) Specifies that the output is restricted to the last *number* of entries. Range is 1 to 210.
first *number*	(Optional) Specifies that the output is restricted to the first *number* of entries. Range is 1 to 210.

Command Default

No instance ID specified displays IS-IS adjacencies for all the IS-IS instances.

Both Level 1 and Level 2 are configured if no level is specified.

Displays all types of route calculation (not just fspf, ispf and prc).

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis spf-log** command:

```
RP/0/RP0:hostname# show isis spf-log

      IS-IS 1 Level 1 IPv4 Unicast Route Calculation Log
                  Time  Total Trig
 Timestamp   Type (ms)  Nodes Count First Trigger LSP Triggers
 ----------- ---- ----  ----- ----- ----- ------- --- --------
 --- Thurs Aug 19 2004 ---
 12:00:50.787  FSPF  1    1     3   ensoft-grs7.00-00 LSPHEADER TLVCODE
 12:00:52.846  FSPF  1    1     1   ensoft-grs7.00-00 LSPHEADER
 12:00:56.049  FSPF  1    1     1   ensoft-grs7.00-00 TLVCODE
 12:01:02.620  FSPF  1    1     2   ensoft-grs7.00-00 NEWADJ LINKTLV

      IS-IS 1 Level 1 IPv4 Unicast Route Calculation Log
                  Time  Total Trig
 Timestamp   Type (ms)  Nodes Count First Trigger LSP Triggers
 ----------- ---- ----  ----- ----- ----- ------- --- --------
 --- Mon Aug 19 2004 ---
 12:00:50.790  FSPF  0    1     4   ensoft-grs7.00-00 LSPHEADER TLVCODE
 12:00:54.043  FSPF  1    1     2   ensoft-grs7.00-00 NEWADJ LSPHEADER
 12:00:55.922  FSPF  1    2     1   ensoft-grs7.00-00 NEWLSPO
 12:00:56.724  FSPF  1    13    1   ensoft-grs7.00-00 NEWLSPO
```

This table describes the significant fields shown in the display.

Table 53: show isis spf-log ipv4 unicast Field Descriptions

Field	Description
Level	IS-IS level of the router.
Timestamp	Time when the SPF calculation started.
Duration	Number of milliseconds taken to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Trig Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. Depending on the configuration of the **spf-interval** command, a router may wait for a fixed period of time before running a router calculation. This count denotes the number of triggering events that occurred while the router was waiting to run the calculation. For a full description of the triggering events, see *List of Triggers*.

Field	Description
First Trigger LSP	LSP ID stored by the router whenever a full SPF calculation is triggered by the arrival of a new LSP. The LSP ID can suggest the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the first received LSP is remembered.
Triggers	List of all reasons that triggered a full SPF calculation. For a list of possible triggers, see *List of Triggers*.

This table lists triggers of a full SPF calculation.

Table 54: List of Triggers

Trigger	Description
PERIODIC	Runs a full SPF calculation very 15 minutes.
NEWLEVEL	Configured new level (using is-type) on this router.
RTCLEARED	Cleared IS-IS topology on the router.
MAXPATHCHANGE	Changed IP maximum parallel path.
NEWMETRIC	Changed link metric.
ATTACHFLAG	Changed Level 2 Attach bit.
ADMINDIST	Configured another administrative distance for the IS-IS instance on this router.
NEWADJ	Created a new adjacency to another router.
DELADJ	Deleted adjacency.
BACKUP	Installed backup route.
SEEDISPF	Seed incremental SPF.
NEXTHOP	Changed IP next-hop address.
NEWLSP0	New LSP 0 appeared in the topology.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	Changed important LSP header fields.
TLVCODE	Type, length, and value (TLV) objects code mismatch, indicating that different TLV objects are included in the newest version of an LSP.
LINKTV	Changed Link TLV content.
PREFIXTLV	Changed Prefix TLV content.
AREAADDRTLV	Changed Area address TLV content.
IP ADDRTLV	Changed IP address TLV content.

Trigger	Description
TUNNEL	Changed RRR tunnel.

The following is sample output from the **show isis spf-log** command with the **first** keyword specified:

```
RP/0/RP0:hostname# show isis spf-log first 2

    IISIS isp Level 1 IPv4 Unicast Route Calculation Log
                 Time  Total Trig
Timestamp   Type (ms)  Nodes Count First Trigger LSP   Triggers
  Mon Aug 16 2004
19:25:35.140  FSPF  1    1     1             12a5.00-00 NEWLSP0
19:25:35.646  FSPF  1    1     1                         NEWADJ


   IISIS isp Level 2  IPv4 Unicast Route Calculation Log
                 Time  Total Trig
Timestamp   Type (ms)  Nodes Count First Trigger LSP   Triggers
  Mon Aug 16 2004
19:25:35.139  FSPF  1    1     1             12a5.00-00 NEWLSP0
19:25:35.347  FSPF  1    1     2             12a5.00-00 NEWSADJ TLVCODE
```

This table describes the significant fields shown in the display.

Table 55: show isis spf-log first Field Descriptions

Field	Description
Level	IS-IS level of the router.
Timestamp	Time at which the SPF calculation started.
Type	Type of route calculation. The possible types are incremental SPF (iSPF), full SPF (FSPF), or partial route calculation (PRC).
Time (ms)	Number of milliseconds taken to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Trig Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. Depending on the configuration of the **spf-interval** command, a router may wait for a fixed period of time before running a router calculation. This count denotes the number of triggering events that occurred while the router was waiting to run the calculation. For a full description of the triggering events, see *List of Triggers*.
First Trigger LSP	LSP ID stored by the router whenever a full SPF calculation is triggered by the arrival of a new LSP. The LSP ID can suggest the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the first received LSP is remembered.

Field	Description
Triggers	List of all reasons that triggered a full SPF calculation. For a list of possible triggers, see *List of Triggers*.

The following is sample output from the **show isis spf-log** command with the **detail** keyword specified:

```
RP/0/RP0:hostname#show isis spf-log detail

    IISIS isp Level 1 IPv4 Unicast Route Calculation Log
                 Time  Total Trig
Timestamp   Type (ms)  Nodes Count First Trigger LSP   Triggers
  Mon Aug 16 2004
19:25:35.140  FSPF  1    1     1             12a5.00-00 NEWLSP0
  Delay:              51ms (since first trigger)
  SPT Calculation
    CPU Time:         0ms
    Real Time:        0ms
  Prefix Updates
    CPU Time:         1ms
    Real Time:        1ms
  New LSP Arrivals:    0
  Next Wait Interval: 200ms
                            Results
                       Reach Unreach Total
   Nodes:                  1       0     1
   Prefixes (Items)
     Critical Priority:    0       0     0
     High Priority:        0       0     0
     Medium Priority       0       0     0
     Low Priority          0       0     0

     All Priorities        0       0     0
   Prefixes (Routes)
     Critical Priority:    0       -     0
     High Priority:        0       -     0
     Medium Priority       0        -    0
     Low Priority:         0        -    0

     All Priorities        0        -    0
```

This table describes the significant fields shown in the display.

Table 56: show isis spf-log detail Field Descriptions

Field	Description
Level	IS-IS level of the router.
Timestamp	Time at which the SPF calculation started.
Type	Type of route calculation. The possible types are incremental SPF (iSPF), full SPF (FSPF), or partial route calculation (PRC).
Time (ms)	Number of milliseconds taken to complete this SPF run. Elapsed time is wall clock time, not CPU time.

Field	Description
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Trig Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. Depending on the configuration of the **spf-interval** command, a router may wait for a fixed period of time before running a router calculation. This count denotes the number of triggering events that occurred while the router was waiting to run the calculation. For a full description of the triggering events, see *List of Triggers*.
First Trigger LSP	LSP ID stored by the router whenever a full SPF calculation is triggered by the arrival of a new LSP. The LSP ID can suggest the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the first received LSP is remembered.
Triggers	List of all reasons that triggered a full SPF calculation. For a list of possible triggers, see *List of Triggers*.
Delay	Two different delays exist: **1.** The delay between the time when the route calculation was first triggered and the time when it was run. **2.** The delay between the end of the last route calculation and the start of this one. This is used to verify that the SPF-interval timers are working correctly, and is only reported for calculations after the first delay.
CPU Time	Two different CPU times exist: **1.** CPU time (in milliseconds) taken to calculate the shortest path tree (SPT). **2.** CPU time (in milliseconds) taken to perform the prefix updates.
Real Time	Two different real times exist: **1.** Real time (in milliseconds) taken to calculate the shortest path tree (SPT). **2.** Real time (in milliseconds) taken to perform the prefix updates.
New LSP Arrivals	Number of LSP arrivals since the start of this route calculation.
Next Wait Interval	Enforced delay until the next route calculation can be run, based on the **spf-interval** command configuration.
Reach	Number of reachable nodes or prefixes.
Unreach	Number of unreachable nodes or prefixes.
Total	Total number of nodes or prefixes at various priorities.

show isis statistics

To display Intermediate System-to-Intermediate System (IS-IS) traffic counters, use the **show isis statistics** command.

show isis [**instance** *instance-id*] **statistics** [*type interface-path-id*]

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS traffic statistics for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No instance ID specified displays IS-IS traffic statistics for all the IS-IS instances.

IS-IS traffic statistics are displayed for all interfaces.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **show isis statistics** command displays IS-IS traffic counters for the specified interface or all traffic counters if no interface is specified.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis statistics** command that shows all traffic counters:

```
RP/0/RP0:hostname#show isis statistics
IS-IS isp statistics:
    Fast PSNP cache (hits/tries): 164115/301454
    Fast CSNP cache (hits/tries): 41828/43302
    Fast CSNP cache updates: 2750
    LSP checksum errors received: 0
    LSP Dropped: 1441
    SNP Dropped: 1958
    UPD Max Queue size: 2431
    Average transmit times and rate:
```

```
  Hello:          0 s,     987947 ns,          4/s
  CSNP:           0 s,    1452987 ns,          0/s
  PSNP:           0 s,    1331690 ns,          0/s
  LSP:            0 s,    1530018 ns,          1/s
Average process times and rate:
  Hello:          0 s,     874584 ns,         41/s
  CSNP:           0 s,     917925 ns,         29/s
  PSNP:           0 s,    1405458 ns,          0/s
  LSP:            0 s,    4352850 ns,          0/s
Level-1:
  LSPs sourced (new/refresh): 3376/2754
  IPv4 Unicast
    SPF calculations           : 527
    ISPF calculations          : 0
    Next Hop Calculations      : 13
    Partial Route Calculations : 1
Level-2:
  LSPs sourced (new/refresh): 4255/3332
  IPv4 Unicast
    SPF calculations           : 432
    ISPF calculations          : 0
    Next Hop Calculations      : 8
    Partial Route Calculations : 0
Interface TenGigE0/1/0/1.1:
Level-1 Hellos (sent/rcvd): 22398/25633
Level-1 DR Elections      : 66
Level-1 LSPs (sent/rcvd)  : 246/7077
Level-1 CSNPs (sent/rcvd) : 0/33269
Level-1 PSNPs (sent/rcvd) : 22/0
Level-1 LSP Flooding Duplicates  : 25129
Level-2 Hellos (sent/rcvd): 22393/67043
Level-2 DR Elections      : 55
Level-2 LSPs (sent/rcvd)  : 265/437
Level-2 CSNPs (sent/rcvd) : 0/86750
Level-2 PSNPs (sent/rcvd) : 0/0
Level-2 LSP Flooding Duplicates  : 78690
```

This table describes the significant fields shown in the display.

Table 57: show isis statistics Field Descriptions

Field	Description
Fast PSNP cache (hits/tries)	Number of successful lookups (hits) along with the number of lookup attempts (tries). To save time or processing power when receiving multiple copies of the same LSP, IS-IS attempts to look up incoming LSPs to see if they have been received recently.
Fast CSNP cache (hits/tries)	Number of successful lookups (hits) along with the number of lookup attempts (tries). To reduce CSNP construction time, IS-IS maintains a cache of CSNPs and attempts to look up CSNP in this cache before transmission on the interface.
Fast CSNP cache updates	Number of times the CSNP cache has been updated since the last clearing of statistics. The cache is updated on LSP addition or removal from the database.
LSP checksum errors received	Number of internal checksum errors received in LSPs.

Field	Description
IIH (LSP/SNP) dropped	Number of hello, LSP, and SNP messages dropped.
IIH (UPD) Max Queue size	Maximum number of queued packets.
Average transmit times and rate	Average time taken to transmit the pdu type across all interfaces and the corresponding rate at which the pdu type is being transmitted.
Average process times and rate	Average time taken to process an incoming pdu type across all interfaces and the corresponding rate at which the pdu type is being received.
LSPs sourced (new/refresh)	Number of LSPs this IS-IS instance has created or refreshed. To find more details on these LSPs, use the **show isis lsp-log** command.
SPF calculations	Number of shortest path first (SPF) calculations. SPF calculations are performed only when the topology changes. They are not performed when external routes change. The interval at which SPF calculations are performed is configured using the **spf-interval** command.
iSPF calculations	Number of incremental shortest path first (iSPF) calculations. iSPF calculations are performed only when ISPF has been configured in the isis address family configuration submode.
Partial Route Calculations	Number of partial route calculations (PRCs). PRCs are processor intensive. Therefore, it may be useful to limit their number, especially how often a PRC is done, especially on slower networking devices. Increasing the PRC interval reduces the processor load on the router, but might slow the rate of convergence. The interval at which PRC calculations are performed is configured using the **spf-interval** command.
Level-(1/2) (LSPs/CSNPs/PSNPs/Hellos) (sent/rcvd)	Number of LSPs, Complete Sequence Number Packets (CSNPs), Partial Sequence Number Packets (PSNPs), and hello packets sent or received on this interface.
PTP Hellos (sent/rcvd)	Point-to-point (PTP) hellos sent and received.
LSP Retransmissions	Total number of retransmissions on each IS-IS LSP on a point-to-point interface. The LSP retransmission interval can be configured using the **retransmit-throttle-interval** command.
Level-(1.2) DRElections	Total number of Designated Intermediate System elections that have taken place. These counts are maintained on an individual level basis.
LSP Flooding Duplicates	Number of duplicate LSPs filtered from flooding to the neighbor. In case of parallel interfaces to the same neighbor, IS-IS optimizes the flooding by avoiding sending the same LSP copy on other interfaces.

show isis topology

To display a list of connected Intermediate System-to-Intermediate System (IS-IS) routers in all areas, use the **show isis topology** command.

show isis [**instance instance-id**] [[{**ipv4** | **afi-all**}] [{**unicast** | [**topology** {**all** | **topo-name**}] | **safi-all**}]] | **summary** | **level** {**1** | **2**} [**systemid system-id**] [**detail**]

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS topology for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
afi-all	(Optional) Specifies all address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
topology *topo-name*	(Optional) Specifies topology table information and name of the topology table.
safi-all	(Optional) Specifies all secondary address prefixes.
summary	(Optional) Displays a brief list of the IS-IS topology.
level { **1** | **2** }	(Optional) Displays the IS-IS link-state topology for Level 1 or Level 2 independently.
systemid *system-id*	(Optional) Displays the information for the specified router only.
detail	(Optional) Displays detailed information on the IS-IS topology.

Command Default

No instance ID specified displays a list of connected routers in all areas for all the IS-IS instances.

Both Level 1 and Level 2 is configured if no level is specified.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show isis topology** command to verify the presence and connectivity among all routers in all areas.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis topology** command:

```
RP/0/RP0:hostname# show isis topology

IS-IS isp paths to (Level-1) routers
    System Id       Metric  Next-hop Interface       SNPA
    ensoft-5        10      ensoft-5        PO0/4/0/1       *PtoP*
    ensoft-5        10      ensoft-5        TenGigE0/5/0/0  0003.6cff.0680
    ensoft-11       --

    IS-IS isp paths to (Level-2) routers
    System Id       Metric  Next-hop Interface       SNPA
    ensoft-5        10      ensoft-5        PO0/4/0/1       *PtoP*
    ensoft-5        10      ensoft-5        TenGigE0/5/0/0  0003.6cff.0680
    ensoft-11       --
```

This table describes the significant fields shown in the display.

Table 58: show isis topology ipv4 unicast Field Descriptions

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
Metric	Metric assigned to the link and used to calculate the cost from each router using the links in the network to other destinations. Range is 1 to 16777214. Default is 1 to 63 for narrow metric and 1 to 16777214 for wide metric. 0 is set internally if no metric has been specified by the user.
Next-hop	Address of the next-hop.
Interface	Interface used to reach the neighbor.
SNPA	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.

The following is sample output from the **show isis topology** command with the **summary** keyword specified:

```
RP/0/RP0:hostname# show isis topology summary

IS-IS 10 IS Topology Summary IPv4 Unicast
                          L1                          L2
                Reach  UnReach  Total      Reach  UnReach  Total
               ------- ------- -------    ------- ------- -------
Router nodes:        1       1       2          1       1       2
Pseudo nodes:        0       0       0          0       0       0

 Total nodes:        1       1       2          1       1       2
```

This table describes the significant fields shown in the display.

Table 59: show isis topology summary Field Descriptions

Field	Description
L1/L2	IS-IS level of the router.
Reach	Number of router nodes or pseudonodes that are reachable.
UnReach	Number of router nodes or pseudonodes that are unreachable.
Total	Total number of reachable and unreachable nodes.

show isis protocol

To display summary information about an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis protocol** command.

show isis [**instance** *instance-id*] **protocol**

Syntax Description

instance *instance-id*	(Optional) Displays the IS-IS adjacencies for the specified IS-IS instance only. • The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Command Default

No instance ID specified displays IS-IS adjacencies for all the IS-IS instances.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis protocol** command:

```
RP/0/RP0:hostname# show isis protocol

IS-IS Router: isp
      System Id: 0001.0000.0011
      IS Levels: level-1-2
      Manual area address(es):
        49

      Routing for area address(es):
        49
      Non-stop forwarding: Cisco Proprietary NSF Restart enabled
      Process startup mode: Cold Restart
      Topologies supported by IS-IS:
        IPv4 Unicast
          Level-1 iSPF status: Dormant (awaiting initial convergence)
          Level-2 iSPF status: Dormant (awaiting initial convergence)
          No protocols redistributed
          Distance: 115
      Interfaces supported by IS-IS:
        Loopback0 is running passively (passive in configuration)
        TenGigE 0/4/0/1 is running actively (active in configuration)
        TenGigE 0/5/0/1 is running actively (active in configuration)
```

This table describes the significant fields shown in the display.

Table 60: show isis protocol Field Descriptions

Field	Description
System ID:	Dynamic hostname of the system. The hostname is specified using the **hostname** command. If the dynamic hostname is not known or **hostname dynamic disable** command has been executed, the 6-octet system ID is used.
IS Levels:	IS-IS level of the router.
Manual area address(es)	Area addresses that are manually configured.
Routing for areaaddress(es)	Area addresses for which this router provides the routing.
Non-stop forwarding:	Status and name of nonstop forwarding (NSF).
Process startup mode:	Mode in which the last process startup occurred. Valid modes are: • Cisco Proprietary NSF Restart • IETF NSF Restart • Cold Restart
iSPF status:	State of incremental shortest path first (iSPF) configuration for this IS-IS instance. Four states exist: Disabled if iSPF has not been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. Dormant if iSPF has been configured but is awaiting initial convergence before initializing. Awake if iSPF has been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. Active if IS-IS is ready to consider using the iSPF algorithm whenever a new route calculation needs to be run.
No protocols redistributed:	No redistributed protocol information exists to be displayed.
Distance:	Administrative distance for this protocol.

shutdown (IS-IS)

To disable the Intermediate System-to-Intermediate System (IS-IS) protocol on a particular interface, use the **shutdown** command in interface configuration mode. To re-enable the IS-IS protocol, use the **no** form of this command.

shutdown
no shutdown

Command Default

IS-IS protocol is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example disables the IS-IS protocol on Ten-Gigabit Ethernet interface 0/1/0/1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE0/1/0/1
RP/0/RP0:hostname(config-isis-if)# shutdown
```

single-topology

To configure the link topology for IP Version 4 (IPv4), use the **single-topology** command in address family configuration mode. To remove the **single-topology** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

single-topology
no single-topology

Command Default

Performs in multitopology mode in which independent topology for IPv4 is running in a single area or domain.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

All interfaces must be configured with the identical set of network protocols, and all routers in the IS-IS area (for Level 1 routing) or the domain (for Level 2 routing) must support the identical set of network layer protocols on all interfaces.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to enable single-topology mode for IPv4:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# net 49.0000.0000.0001.00
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# single-topology
```

snmp-server traps isis

snmp-server traps isis {**all** | *traps set*}
no snmp-server traps isis {**all** | *traps set*}

Syntax Description

all	Specifies all IS-IS SNMP server traps.
traps set	Specify any set of trap names.

Command Modes

Router configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

```
RP/0/RP0:hostname(config)# snmp-server traps isis

  adjacency-change                 isisAdjacencyChange
  all                              Enable all IS-IS traps
  area-mismatch                    isisAreaMismatch
  attempt-to-exceed-max-sequence   isisAttemptToExceedMaxSequence
  authentication-failure           isisAuthenticationFailure
  authentication-type-failure      isisAuthenticationTypeFailure
  corrupted-lsp-detected           isisCorruptedLSPDetected
  database-overload                isisDatabaseOverload
  id-len-mismatch                  isisIDLenMismatch
  lsp-error-detected               isisLSPErrorDetected
  lsp-too-large-to-propagate       isisLSPTooLargeToPropagate
  manual-address-drops             isisManualAddressDrops
  max-area-addresses-mismatch      isisMaxAreaAddressesMismatch
  orig-lsp-buff-size-mismatch      isisOrigLSPBuffSizeMismatch
  own-lsp-purge                    isisOwnLSPPurge
  protocols-supported-mismatch     isisProtocolsSupportedMismatch
  rejected-adjacency               isisRejectedAdjacency
  sequence-number-skip             isisSequenceNumberSkip
  version-skew                     isisVersionSkew

RP/0/RP0:hostname(config)#snmp-server traps isis all
```

spf-interval

To customize IS-IS throttling of shortest path first (SPF) calculations, use the **spf-interval** command in address family configuration mode. To restore default values, use the **no** form of this command.

spf-interval [{**initial-wait** *initial* | **secondary-wait** *secondary* | **maximum-wait** *maximum*}] **. . .** [**level** {**1** | **2**}]
no spf-interval [[{**initial-wait** *initial* | **secondary-wait** *secondary* | **maximum-wait** *maximum*}] **. . .**] [**level** {**1** | **2**}]

Syntax Description

initial-wait *initial*	Initial SPF calculation delay (in milliseconds) after a topology change. Range is 0 to 120000.
secondary-wait *secondary*	Hold time between the first and second SPF calculations (in milliseconds). Range is 0 to 120000.
maximum-wait *maximum*	Maximum interval (in milliseconds) between two consecutive SPF calculations. Range is 0 to 120000.
level { **1** | **2** }	(Optional) Enables the SPF interval configuration for Level 1 or Level 2 independently.

Command Default

initial-wait *initial* : 50 milliseconds

secondary-wait *secondary* : 200 milliseconds

maximum-wait *maximum* : 5000 milliseconds

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

Use the **spf-interval** command to control how often the software can perform the SPF calculation. The SPF calculation is processor intensive. Therefore, it may be useful to limit how often this calculation is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but potentially slows the rate of convergence.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to set the initial SPF calculation delay to 10 milliseconds and the maximum interval between two consecutive SPF calculations to 5000 milliseconds:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# spf-interval initial-wait 10 maximum-wait 5000
```

spf prefix-priority (IS-IS)

To assign a priority to an ISIS prefix for customizing the RIB update sequence, use the**spf prefix-priority** command in address family configuration mode. To restore default values, use the **no** form of this command.

spf prefix-priority [**level** {**1** | **2**}] {**critical** | **high** | **medium**} {*access-list-name* | **tag** *tag*}
no spf prefix-priority [**level** {**1** | **2**}] {**critical** | **high** | **medium**} [{*access-list-name* | **tag** *tag*}]

Syntax Description

level { **1** | **2** }	(Optional) Enables the assignment of a priority to Level 1 or Level 2 independently.
critical	Assigns a critical priority.
high	Assigns a high priority.
medium	Assigns a medium priority.
access-list-name	Name of an access list.
tag *tag*	Specifies a tag to indicate priority. The *tag* argument range is 1 to 4294967295.

Command Default

By default, IPv4 prefixes with a length of 32 are given medium priority. The remaining prefixes are given low priority.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **spf prefix-priority** command to change the sequence of prefix updates to the RIB after an SPF is run. ISIS installs prefixes in the RIB according to the following priority order:

Critical > High > Medium > Low

The **spf prefix-priority** command supports prefix lists for the first three priorities. The unmatched prefixes are updated with low priority.

If a **spf prefix-priority** is specified, the default behavior of prioritizing length 32 prefixes for IPv4 , as **medium** is disabled.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to set the prefix priorities:

```
RP/0/RP0:hostname(config)# ipv4 prefix-list isis-critical-acl
```

```
RP/0/RP0:hostname(config-ipv4_pfx)# 10 permit 0.0.0.0/0 eq 32
!
RP/0/RP0:hostname(config)# ipv4 prefix-list isis-med-acl
RP/0/RP0:hostname(config-ipv4_pfx)# 10 permit 0.0.0.0/0 eq 29
!
RP/0/RP0:hostname(config)# ipv4 prefix-list isis-high-acl
RP/0/RP0:hostname(config-ipv4_pfx)# 10 permit 0.0.0.0/0 eq 30
!
RP/0/RP0:hostname(config)# router isis ring
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# spf prefix-priority critical isis-critical-acl
RP/0/RP0:hostname(config-isis-af)# spf prefix-priority high isis-high-acl
RP/0/RP0:hostname(config-isis-af)# spf prefix-priority medium isis-med-acl
```

summary-prefix (IS-IS)

To create aggregate addresses for the Intermediate System-to-Intermediate System (IS-IS) protocol, use the **summary-prefix** command in address family configuration mode. To restore the default behavior, use the **no** form of this command.

Syntax Description

address	Summary address designated for a range of IPv4 addresses. The *address* argument must be in four-part, dotted-decimal notation.
/ *prefix-length*	Length of the IPv4 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
level { **1** | **2** }	(Optional) Redistributes routes into Level 1 or Level 2 and summarizes them with the configured address and mask value.
tag *tag*	Sets a tag value. The value range is 1- 4294967295.

Command Default

All redistributed routes are advertised individually.

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more-specific routes. Use the **summary-prefix** command to help reduce the size of the routing table.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database. It also helps ensure stability, because a summary advertisement depends on many more specific routes. If one more-specific route flaps, in most cases, this flap does not cause a flap of the summary advertisement.

The drawback of summary addresses is that other routes might have less information to calculate the most optimal routing table for all individual destinations.

Note When IS-IS advertises a summary prefix, it automatically inserts the summary prefix into the IP routing table but labels it as a “discard” route entry. Any packet that matches the entry is discarded to prevent routing loops. When IS-IS stops advertising the summary prefix, the routing table entry is removed.

Task ID

Task ID	Operations
isis	read, write

Examples

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-af)# redistribute ospf 2 level-2
RP/0/RP0:hostname(config-isis-af)# summary-prefix 10.10.10.10 level-2
RP/0/RP0:hostname(config-isis-af)# summary-prefix 10.10.10.10
```

suppressed

To allow an IS-IS interface to participate in forming adjacencies without advertising connected prefixes in the system link-state packets (LSPs), use the **suppressed** command in interface configuration mode. To enable advertising connected prefixes, use the **no** form of this command.

suppressed
no suppressed

Command Default

Interface is active.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **suppressed** command to reduce the number of routes that IS-IS has to maintain, improving convergence times after an isolated failure. Improvement is noticeable if the command is used widely throughout the network. Other routers in the domain do not install routes to the affected connected prefixes.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to disable the advertisement of connected prefixes on TenGigE interface 0/1/0/1:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/1/0/1
RP/0/RP0:hostname(config-isis-if)# suppressed
```

tag (IS-IS)

To associate and advertise a tag with the prefix of an IS-IS interface, use the **tag** command in interface address family configuration mode. To restore the default behavior, use the **no** form of this command.

tag *tag*
no tag [*tag*]

Syntax Description

tag	Interface tag. Range is 1 to 4294967295.

Command Default

Default is that no tag is associated and advertised.

Command Modes

Interface address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to associate and advertise an interface tag:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/3/0/0
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-if-af)# tag 234
```

topology-id

To differentiate one topology in the domain from another while configuring a multicast routing table, use the **topology-id** command in Intermediate System-to-Intermediate System (IS-IS) address family configuration submode. To disable the topology use the **no** form of the command.

topology-id *isis-multicast-topology-id-number*
no topology-id *isis-multicast-topology-id-number*

Syntax Description

isis-multicast-topology-id-number	ID number for a specific IS-IS multicast topology. Range is 6 to 4095.

Command Default

No topology is associated with a routing table by default.

Command Modes

IS-IS address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to differentiate a topology from another in the multicast routing table in IS-IS routing:

```
RP/0/RP0:hostname(config)# router  isis isp
RP/0/RP0:hostname(config-isis)# address-family ipv4 multicast topology   green
RP/0/RP0:hostname(config-isis-af)# topology-id 2666
```

trace (IS-IS)

To set the the IS-IS buffer size, use the **trace** command in router configuration mode. To return to the default value, use the **no** form of this command.

trace [{**detailed** | **severe** | **standard**}] *max-trace-entries*
no trace [{**detailed** | **severe** | **standard**}]

Syntax Description

detailed	Specifies the buffer size for detailed traces. Range is
severe	Specifies the buffer size for severe traces. Range is
standard	Specifies the buffer size for standard traces. Range is
max-trace-entries	Sets the maximum number of trace entries. Range is 1-20000

Command Default

None

Command Modes

Router IS-IS configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operation
isis	read, write

Examples

The following example shows how to set the isis buffer size for severe traces to 1200:

```
RP/0/RP0:hostname(config)#router isis isp
RP/0/RP0:hostname(config-isis)#trace sever 1200
```

L2Xconnect/VLAN/EVC Command Reference

This chapter describes the commands to configure L2Xconnect/VLAN/EVC.

Note Refer *OTN and DWDM Configuration Guide for Cisco NCS 4000 Series*, for LANPHY and Ethernet terminated OTN controller configuration procedures.

l2transport (Ethernet)

To enable Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode, use the **l2transport** command in interface configuration mode for an Ethernet interface. To disable Layer 2 transport port mode on an Ethernet interface, use the **no** form of this command.

l2transport

no l2transport

Command Default

None.

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you issue the l2transport command in interface configuration mode, the CLI prompt changes to "config-if-l2," indicating that you have entered the Layer 2 transport configuration submode. In the following sample output, the question mark (?) online help function displays all the commands available under Layer 2 transport configuration submode for an Ethernet interface:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/5/2
RP/0/RP0:hostname(config-if)# l2transport
RP/0/RP0:hostname(config-if-l2)# ?
  commit          Commit the configuration changes to running
  describe        Describe a command without taking real actions
  do              Run an exec command
  exit            Exit from this submode
  no              Negate a command or set its defaults
  service-policy  Configure QoS Service policy
  show            Show contents of configuration
RP/0/RP0:hostname(config-if-l2)#
```

Note The l2transport command is mutually exclusive with any Layer 3 interface configuration

Task ID

Task ID	Operation
l2vpn	read, write

Examples

The following example shows how to enable Layer 2 transport port mode on an Ethernet interface and enter Layer 2 transport configuration mode:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/2/0/2
RP/0/RP0:hostname(config-if)# l2transport
RP/0/RP0:hostname(config-if-l2)#
```

The following example shows how to use the l2transport keyword in the interface command:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/2.10 l2transport
RP/0/RP0:hostname(config-if)# encapsulation dot1q 200
RP/0/RP0:hostname(config-if-l2)#commit
```

The following example shows how to use the l2transport command on an Ethernet subinterface:

Note Ensure that the l2transport command is applied on the same line as the interface command for the Ethernet subinterface.

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#interface TenGigE0/5/0/1.1 l2transport
RP/0/RP0:hostname(config-subif)#encapsulation dot1q 100
RP/0/RP0:hostname(config-subif)#commit
RP/0/RP0:hostname(config-subif)#end

RP/0/RP0:hostname#sh run | begin TenGigE0/5/0/1
Thu Dec  3 10:15:40.916 EST Building configuration...
interface TenGigE0/5/0/1
 mtu 1500
!
interface TenGigE0/5/0/1.1 l2transport
encapsulation dot1q 100
interface TenGigE0/5/0/2
 shutdown
!
!
```

Note To configure l2transport on an Ethernet subinterface, ensure that the main interface is configured as a Layer 3 interface.

dot1q tunneling ethertype

To configure the Ethertype, used by peer devices when implementing QinQ VLAN tagging, to be 0x9100, use the **dot1q tunneling ethertype** command in the interface configuration mode for an Ethernet interface. To return to the default Ethertype configuration (0x8100), use the **no** form of this command.

dot1q tunneling ethertype {*0x9100* | *0x9200* }

no dot1q tunneling ethertype

Syntax Description

0x9100	Sets the Ethertype value to 0x9100.
0x9200	Sets the Ethertype value to 0x9200.

Command Default

The Ethertype field used by peer devices when implementing QinQ VLAN tagging is either 0x8100 or 0x8200.

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The dot1q tunneling ethertype command can be applied to a main interface. When applied to the main interface, it changes the subinterfaces, that have been configured with an encapsulation dot1q second-dot1q command, under that main interface.

This command changes the outer VLAN tag from 802.1q Ethertype 0x8100 to 0x9100 or 0x9200.

Task ID

Task ID	Operation
vlan	read, write

Examples

The following example shows how to configure the Ethertype to 0x9100:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/2
RP/0/RP0:hostname(config-if)# dot1q tunneling ethertype 0x9100
```

The following example shows how to configure the Ethertype to 0x9200:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/6
RP/0/RP0:hostname(config-if)# dot1q tunneling ethertype 0x9200
```

encapsulation default

To configure the default sub interface on a port, use the **encapsulation default** command in the interface configuration mode. To delete the default sub interface on a port, use the **no** form of this command.

encapsulation default

no encapsulation default

Command Default No default sub interface is configured on the port.

Command Default No default sub interface is configured on the port.

Command Modes Interface configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If the default sub interface is the only one configured on a port, the encapsulation default command matches all ingress frames on that port. If the default sub interface is configured on a port that has other non-default sub interfaces, the encapsulation default command matches frames that are unmatched by those non-default sub interfaces (anything that does not meet the criteria of other sub interfaces on the same physical interface falls into this sub interface).

Only a single default sub interface can be configured per interface. If you attempt to configure more than one default sub interface per interface, the encapsulation default command is rejected.

Only one encapsulation command must be configured per sub interface.

Example

The following example shows how to configure a sub interface on a port:

```
RP/0/RP0:hostname(config-subif)# encapsulation default
```

encapsulation dot1ad dot1q

To define the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate sub interface, use the **encapsulation dot1ad dot1q** command in sub interface configuration mode.

To delete the matching criteria to map single-tagged 802.1ad frames ingress on an interface to the appropriate sub interface, use the **no** form of this command.

encapsulation dot1ad *vlan-id* **dot1q** {*vlan-id* }

no encapsulation dot1ad *vlan-id* **dot1q** {*vlan-id* }

Syntax Description

dot1ad	Sets the Ethertype value to 0x9100.
dot1q	Sets the Ethertype value to 0x9200.
vlan-id	VLAN ID, integer in the range 1 to 4094. A hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) A comma must be entered to separate each VLAN ID range from the next range.

Command Default

No matching criteria are defined.

Command Modes

sub interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The outer VLAN tag is an 802.1ad VLAN tag, instead of an 802.1Q tag. An 802.1ad tag has an ethertype value of 0x88A8, instead of 0x8100 that 802.1Q uses.

Some of the fields in the 802.1ad VLAN header are interpreted differently per 802.1ad standard. A tunneling ethertype command applied to the main interface does not apply to an 802.1ad sub interface.

An interface with encapsulation dot1ad causes the router to categorize the interface as an 802.1ad interface.

Example

The following example shows how to map single-tagged 802.1ad ingress frames to a sub interface:

```
RP/0/RP0:hostname(config-subif)# encapsulation dot1ad 100 dot1q 20
```

encapsulation dot1q

To define the matching criteria to map 802.1Q frames ingress on an interface to the appropriate sub interface, use the encapsulation dot1q command in the interface configuration mode. To delete the matching criteria to map 802.1Q frames ingress on an interface to the appropriate sub interface, use the **no** form of this command.

encapsulation dot1q *vlan-id* [*,vlan-id [-vlan-id]*] [**exact** *mac-address* | **second-dot1q** *vlan-id*]

encapsulation dot1q *vlan-id*, **untagged**

no encapsulation dot1q

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) Comma must be entered to separate each VLAN ID range from the next range.
exact	(Optional) Prevents matching of frames with more than one tag.
untagged	(Optional) Allows matches for both the single-tag dot1q frames and untagged frames.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Only one encapsulation statement can be applied to a sub interface. Encapsulation statements cannot be applied to main interfaces.

A single encapsulation dot1q statement specifies matching for frames with a single VLAN ID; a range of VLAN IDs; or a single VLAN ID or untagged.

Task ID

Task ID	Operation
vlan	read, write

The following example shows how to map 802.1Q frames ingress on an interface to the appropriate sub interface:

```
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
```

encapsulation dot1q second-dot1q

To define the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate sub interface, use the **encapsulation dot1q second-dot1q** command in the interface configuration mode. To delete the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate sub interface, use the **no** form of this command.

encapsulation dot1q *vlan-id* **second-dot1q** { **any** | *vlan-id* [*,vlan-id [-vlan-id]*] [**exact** | **ingress source-mac** *mac-address*] }

no encapsulation dot1q *vlan-id* **second-dot1q** { **any** | *vlan-id* [*,vlan-id [-vlan-id]*] [**exact** | **ingress source-mac** *mac-address*] }

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) Comma must be entered to separate each VLAN ID range from the next range.
second-dot1q	(Optional) Specifies IEEE 802.1Q VLAN tagged packets.
any	Any second tag in the range 1 to 4094.
exact	(Optional) Ensures that frames with more than two tags do not match.
ingress source-mac	(Optional) Performs MAC-based matching.

Command Default

No matching criteria are defined.

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The criteria for this command are: the outer tag must be unique and the inner tag may be a single VLAN, a range of VLANs or lists of the previous two.

QinQ sub interface, allows single or range on second-dot1q.

Only one encapsulation command must be configured per sub interface.

Task ID

Task ID	Operation
vlan	read, write

Example:

The following example shows how to map 802.1Q frames ingress on an interface to the appropriate sub interface:

```
RP/0/RP0:hostname(config)# interface HundredGigE0/8/0/0.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10 second-dot1q 100
```

encapsulation untagged

To define the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate sub interface, use the **encapsulation untagged** command in the Interface configuration mode. To delete the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate sub interface, use the **no** form of this command.

encapsulation untagged

no encapsulation untagged

Command Default

No matching criteria are defined.

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Only one sub interface per port is allowed to have untagged encapsulation. The reason is to be able to unambiguously map the incoming frames to the sub interface. However, it is possible for a port that hosts an sub interface matching untagged traffic to host other sub interfaces that match tagged frames. Only one encapsulation command may be configured per sub interface.

Only one sub interface may be configured as encapsulation untagged. This interface is referred to as the untagged sub interface or untagged EFP (incase of an L2 interface).

The untagged sub interface has a higher priority than the main interface; all untagged traffic, including L2 protocol traffic, passes through this sub interface rather than the main interface.

Task ID

Task ID	Operation
vlan	read, write

Examples:

The following example shows how to map untagged ingress Ethernet frames to a sub interface:

```
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/2.10 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation untagged
```

rewrite ingress tag

To specify the encapsulation adjustment that is to be performed on the frame ingress to the sub interface, use the **rewrite ingress tag** command in the interface configuration mode. To delete the encapsulation adjustment that is to be performed on the frame ingress to the sub interface, 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** { **1to1** { **dot1q** *vlan-id* | **dot1ad** *vlan-id* } | **2-to-2** { **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id* } } [**symmetric**]

no rewrite ingress tag { **push** { **dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id* } | **pop** { **1** | **2** } | **translate** { **1to1** { **dot1q** *vlan-id* | **dot1ad** *vlan-id* } | **2-to-2** { **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id* } } [**symmetric**]

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094.
push dot1q *vlan-id*	Pushes one 802.1Q tag with vlan-id .
push dot1q *vlan-id* **second-dot1q** *vlan-id*	Pushes a pair of 802.1Q tags in the order first, second.
pop {1 | 2}	One or two tags are removed from the packet. This command can be combined with a push (pop N and subsequent push vlan-id).
translate 1-to-1 dot1q *vlan-id*	Replaces the incoming tag (defined in the encapsulation command) into a different 802.1Q tag at the ingress sub interface.
translate 2-to-2 dot1q *vlan-id* **second-dot1q** *vlan-id*	Replaces the pair of tags defined by the encapsulation command by a pair of VLANs defined by this rewrite.
symmetric	A rewrite operation is applied on both ingress and egress. The operation on egress is the inverse operation as ingress.

Command Default

The frame is left intact on ingress.

Command Modes

Interface configuration mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **symmetric** keyword is accepted only when a single VLAN is configured in encapsulation. If a list of VLANs or a range VLAN is configured in encapsulation, the **symmetric** keyword is accepted only for push rewrite operations; all other rewrite operations are rejected.

The **pop** command assumes the elements being popped are defined by the encapsulation type. The exception case should be drop the packet.

The **rewrite ingress tag translate** command assume the tags being translated from are defined by the encapsulation type. The translation operation requires at least “from” tag in the original packet. If the original packet contains more tags than the ones defined in the “from”, then the operation should be done beginning on the outer tag. Exception cases should be dropped.

Task ID

Task ID	Operation
vlan	read, write

Examples

The following example shows how to specify the encapsulation adjustment that is to be performed on the frame ingress to the sub interface:

```
RP/0/RP0:hostname(config-subif)# rewrite ingress push dot1q 200
```

CFM-EOAM Command Reference

This chapter describes the commands to configure CFM-EOAM.

action capabilities-conflict

To configure what action is taken on an interface when a capabilities-conflict event occurs, use the **action capabilities-conflict** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action capabilities-conflict {**disable** | **efd** | **error-disable-interface** | **log**}
no action capabilities-conflict {**disable** | **efd** | **error-disable-interface** | **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a capabilities-conflict event occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action capabilities-conflict disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a capabilities-conflict event occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
```

```
RP/0/RP0:hostname(config-eoam)# action capabilities-conflict efd
```

The following example shows how to configure that the interface is put into the error-disable state when a capabilities-conflict event occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action capabilities-conflict error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a capabilities-conflict event occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action capabilities-conflict log
```

action critical-event

To configure what action is taken on an interface when a critical-event notification is received from the remote Ethernet OAM peer, use the **action critical-event** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action critical-event {**disable** | **error-disable-interface** | **log**}
no action critical-event {**disable** | **error-disable-interface** | **log**}

Syntax Description

disable	Performs no action on the interface when a critical-event notification is received.
error-disable-interface	Puts the interface into the error-disable state when a critical-event notification is received.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a critical-event notification is received. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a critical-event notification is received.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action critical-event disable
```

The following example shows how to configure that the interface is put into the error-disable state when a critical-event notification is received.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action critical-event error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a critical-event notification is received. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action critical-event log
```

action discovery-timeout

To configure what action is taken on an interface when a connection timeout occurs, use the **action discovery-timeout** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action discovery-timeout {**disable** | **efd error-disable-interface** | **log**}
no action discovery-timeout {**disable** | **efd error-disable-interface** | **log**}

Syntax Description

disable	Performs no action on the interface when a connection timeout occurs.
efd	Puts the line protocol into the down state for an interface when a connection timeout occurs. The state is removed when the session is re-established.
error-disable-interface	Puts the interface into the error-disable state when a connection timeout occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a connection timeout occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a connection timeout occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action discovery-timeout disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a connection timeout occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action discovery-timeout efd
```

The following example shows how to configure that the interface is put into the error-disable state when a connection timeout occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action discovery-timeout error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a connection timeout occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action discovery-timeout log
```

action dying-gasp

To configure what action is taken on an interface when a dying-gasp notification is received from the remote Ethernet OAM peer, use the **action dying-gasp** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action dying-gasp {**disable** | **error-disable-interface** | **log**}
no action dying-gasp {**disable** | **error-disable-interface** | **log**}

Syntax Description

disable	Performs no action on the interface when a dying-gasp notification is received.
error-disable-interface	Puts the interface into the error-disable state when a dying-gasp notification is received.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a dying-gasp notification is received. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a dying-gasp notification is received.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action dying-gasp disable
```

The following example shows how to configure that the interface is put into the error-disable state when a dying-gasp notification is received.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action dying-gasp error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a dying-gasp notification is received. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action dying-gasp log
```

action high-threshold

To configure what action is taken on an interface when a high threshold is exceeded, use the **action high-threshold** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action high-threshold {**disable** | **error-disable-interface** | **log**}
no action high-threshold {**disable** | **error-disable-interface** | **log**}

Syntax Description

disable	(Interface Ethernet OAM configuration only) Performs no action on the interface when a high threshold is exceeded.
error-disable-interface	Puts the interface into the error-disable state when a high threshold is exceeded.
log	Creates a syslog entry when a high threshold is exceeded. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default is that no action is taken when a high threshold is exceeded.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that a syslog entry is created on the interface when a high threshold is exceeded.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action high-threshold log
```

The following example shows how to configure that the interface is put into the error-disable state when a high threshold is exceeded.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action high-threshold error-disable-interface
```

The following example shows how to configure that no action is taken when a high threshold is exceeded. This configuration overrides the Ethernet OAM profile configuration.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action high-threshold disable
```

action session-down

To configure what action is taken on an interface when an Ethernet OAM session goes down, use the **action session-down** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action session-down {**disable** | **efd** | **error-disable-interface** | **log**}
no action session-down {**disable** | **efd** | **error-disable-interface** | **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session goes down.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action session-down disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when an Ethernet OAM session goes down.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
```

```
RP/0/RP0:hostname(config-eoam)# action session-down efd
```

The following example shows how to configure that the interface is put into the error-disable state when an Ethernet OAM session goes down.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action session-down error-disable-interface
```

The following example shows how to configure that a syslog entry is created when an Ethernet OAM session goes down. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action session-down log
```

action session-up

To configure what action is taken on an interface when an Ethernet OAM session is established, use the **action session-up** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action session-up {**disable** | **log**}
no action session-up {**disable** | **log**}

Syntax Description

disable	Performs no action on the interface when an Ethernet OAM session is established.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when an Ethernet OAM session is established. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session is established.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action session-up disable
```

The following example shows how to configure that a syslog entry is created when an Ethernet OAM session is established. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action session-up log
```

action uni-directional link-fault

To configure what action is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer, use the **action uni-directional link-fault** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action uni-directional link-fault {**disable** | **efd** | **error-disable-interface** | **log**}
no action uni-directional link-fault {**disable** | **efd** | **error-disable-interface** | **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command only determines the action taken when a uni-directional link fault notification is received from the peer; it does not affect the action taken when a fault is detected locally.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a link-fault notification is received.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action uni-directional link-fault disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a link-fault notification is received.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action uni-directional link-fault efd
```

The following example shows how to configure that the interface is put into the error-disable state when a link-fault notification is received.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action uni-directional link-fault error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a link-fault notification is received. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# action uni-directional link-fault log
```

action wiring-conflict

To configure what action is taken on an interface when a wiring-conflict event occurs, use the **action wiring-conflict** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of this command.

action wiring-conflict {**disable** | **efd** | **error-disable-interface** | **log**}
no action wiring-conflict {**disable** | **efd** | **error-disable-interface** | **log**}

Syntax Description

disable	Performs no action on the interface when a capabilities-conflict event occurs.
efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
log	(Interface Ethernet OAM configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available only in interface Ethernet OAM configuration mode to override the OAM profile on a specific interface.

Command Default

The default action is to put the interface into error-disable state.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure that no action is performed on the interface when a wiring-conflict event occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action wiring-conflict disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a wiring-conflict event occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
```

```
RP/0/RP0:hostname(config-eoam)# action wiring-conflict efd
```

The following example shows how to configure that a syslog entry is created when a wiring-conflict event occurs.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# action wiring-conflict log
```

The following example shows how to configure that the interface is put into the error-disable state when a wiring-conflict event occurs. This configuration overrides the interface Ethernet OAM profile.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
(config-if-eoam)# action wiring-conflict error-disable-interface
```

aggregate

To configure the size and number of bins into which to aggregate the results of statistics collection, use the **aggregate** command in SLA profile statistics configuration mode.

aggregate { **bins** *count* **width** *width* | **none** }

Syntax Description

bins *count*	Number of bins. The range is 2 to 100.
width *width*	For delay and jitter measurements, the size of each bin in milliseconds (range 1-10000). For loss measurements, the size of each bin in percentage points (range 1-100). In addition, the width must be specified if the number of bins is at least 2, regardless of the type of measurement.
none	No aggregation is performed. All samples are stored individually.

Command Default

For delay measurements, all collected statistics are aggregated into one bin.

For loss measurements, the default is aggregation disabled.

Command Modes

SLA profile statistics configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

Changing the aggregation for a given metric clears all stored data for that metric.

For delay and jitter measurements, the first bin starts at 0, each bin covers a range of values defined by the specified width, except for the last bin which ends at infinity. For example, an aggregate bin count of 4 and a width of 20 for delay measurements yields 4 bins of statistics for these sample ranges:

- Bin 1—Samples with delay ranges 0 to < 20 ms.
- Bin 2—Samples with delay ranges greater than or equal to 20 and < 40 ms.
- Bin 3—Samples with delay ranges greater than or equal to 40 and < 60 ms.
- Bin 4—Samples with delay ranges 60 ms or greater (unbounded).

For synthetic loss measurements, the first bin starts at 0, each bin covers a range of values defined by the specified width, except for the last bin which ends at infinity. For example, an aggregate bin count of 4 and a width of 25 for loss measurements yields 4 bins of statistics for these sample ranges:

- Bin 1—Samples with loss ranges 0 to < 25 percentage points.
- Bin 2—Samples with loss ranges greater than or equal to 25 and < 50 percentage points.
- Bin 3—Samples with loss ranges greater than or equal to 50 and < 75 percentage points.
- Bin 4—Samples with loss ranges greater than or equal to 75 and <100 percentage points.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **aggregate** command:

```
RP/0/RP0:router(config-sla-prof-stat-cfg)# aggregate bins 4 width 20
```

ais transmission

To configure Alarm Indication Signal (AIS) transmission for a Connectivity Fault Management (CFM) domain service, use the **ais transmission** command in CFM domain service configuration mode. To disable AIS transmission in a CFM domain service, use the no form of this command.

ais transmission [{**interval 1s** | **1m**}] [**cos** *cos*]
no ais transmission [{**interval 1s** | **1m**}] [**cos** *cos*]

Syntax Description

interval	(Optional) Interval at which AIS packets are transmitted. Valid values are: • **1s** – Interval of 1 second • **1m** – Interval of 1 minute
cos *cos*	(Optional) Specifies the Class of Service (CoS) for the AIS packets. Valid values are 0 to 7.

Command Default

AIS transmission is disabled by default.

If **interval** is not specified, the default interval is 1 second.

IF **cos** is not specified, the default cos is 6.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command enables AIS for all MEPs in the service. AIS messages are triggered by the following events:

- Detection of a CCM defect.
- Detection of a missing peer MEP (when cross-check is configured).
- Receipt of AIS or LCK messages.
- Detection of interface down events (for down MEPs only).

AIS messages are transmitted in the opposite direction of CCMs and other CFM messages that are sent by the MEP. Therefore, up MEPs send AIS messages out of the interface, whereas down MEPs send AIS messages toward the bridging function.

In addition, AIS messages are sent at a higher maintenance level than other CFM messages sent by the MEP:

- If there is a higher-level MEP on the interface in the same direction (up MEP or down MEP), then the AIS messages are passed internally to this higher level MEP. In this case, no AIS messages are actually transmitted (unless the higher-level MEP is also in a service with AIS transmission configured).
- If there is a MIP on the interface, then AIS messages are sent at the level of the MIP.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure Alarm Indication Signal (AIS) transmission for a CFM domain service:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0:hostname(config-cfm-dmn-svc)# ais transmission interval 1m cos 7
```

ais transmission up

To configure Alarm Indication Signal (AIS) transmission on a Connectivity Fault Management (CFM) interface, use the **ais transmission up** command in interface CFM configuration mode. To disable AIS transmission on an interface, use the no form of this command.

ais transmission up [{**interval 1s** | **1m**}] [**cos** *cos*]
no ais transmission up [{**interval 1s** | **1m**}] [**cos** *cos*]

Syntax Description

interval	(Optional) Interval at which AIS packets are transmitted. Valid values are: • **1s** – Interval of 1 second • **1m** – Interval of 1 minute
cos *cos*	(Optional) Specifies the Class of Service (CoS) for the AIS packets. Valid values are 0 to 7.

Command Default

AIS transmission is disabled by default.

If **interval** is not specified, the default interval is 1 second.

IF **cos** is not specified, each MEP uses its own CoS value, inherited from the interface.

Command Modes

Interface CFM configuration (config-if-cfm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

AIS transmission packets for CFM can be configured only on interfaces with no down MEPs. AIS packets are transmitted only if a MIP exists on the interface and the line protocol state is down. AIS messages are transmitted up, toward the bridging function (same direction as an up MEP sends CCMs), and they are transmitted at the level of the MIP.

If AIS transmission is configured on an interface with any down MEPs, the configuration is ignored, and an error is displayed in the **show ethernet cfm configuration-errors** command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure AIS transmission on a CFM interface.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/2
RP/0/RP0:hostname(config-if)# ethernet cfm
RP/0/RP0:hostname(config-if-cfm)# ais transmission up interval 1m cos 7
```

buckets size

To configure the size of the buckets in which statistics are collected, use the **buckets size** command in the appropriate mode.

buckets size *number* { **probes** }

Syntax Description

number	Specifies the size of each bucket. The number of probes that each buckets may contain. The range is 1 to 100.
probes	Buckets span multiple probes.

Command Default

None

Command Modes

SLA profile statistics configuration mode

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

A bucket represents a time period during which statistics are collected. All the results received during that time period are recorded in the corresponding bucket. If aggregation is enabled, each bucket has its own set of bins and counters, and only results received during the time period represented by the bucket are included in those counters.

There is a separate bucket for each probe. The time period is determined by how long the probe lasts. This command allows you to modify the size of buckets.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **buckets size** command:

```
RP/0/RP0:router(config-sla-prof-stat-cfg)# buckets size 100 probes
```

clear ethernet cfm ccm-learning-database location

To clear the Continuity Check Message (CCM) learning database, use the **clear ethernet cfm ccm-learning-database location** command in EXEC mode.

clear ethernet cfm ccm-learning-database location {**all***node-id*}

Syntax Description

all	Clears the CCM learning database for all interfaces.
node-id	Clears the CCM learning database for the designated node, entered in *r ack*/*slot*/*module* notation.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all the CFM CCM learning databases on all interfaces:

```
RP/0/RP0:hostname# clear ethernet cfm ccm-learning-database location all
```

clear ethernet cfm interface statistics

To clear the counters for an Ethernet CFM interface, use the **clear ethernet cfm interface statistics** command in exec mode.

clear ethernet cfm interface *interface-path-id* **statistics** [**location** {**all** | **location**}]
clear ethernet cfm interface statistics location {**all***node-id*}

Syntax Description

interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	(Optional only when used with a specified interface) Clears MAC accounting statistics for a designated interface or for all interfaces.
all	Clears CFM counters for all interfaces.
node-id	Clears CFM counters for a specified interface, using *rack/slot* notation

Command Default

No default behavior or values

Command Modes

Exec

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all the CFM counters from all interfaces:

```
RP/0/RP0:hostname# clear ethernet cfm interface statistics location all
```

clear ethernet cfm local meps

To clear the counters for all MEPs or a specified MEP, use the **clear ethernet cfm local meps** command in EXEC mode.

clear ethernet cfm local meps {**all** | **domain** *domain-name* {**all** | **service** *service-name* {**all** | **mep-id** *id*}} | **interface** *interface-name* {**all** | **domain** *domain-name*}}

Syntax Description

all	Clears counters for all local MEPs.
domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
mep-id *id*	Maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *interface-name*	String of a maximum of 80 characters that identifies the Ethernet interface.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The following counters are cleared:

- Number of continuity-check messages (CCMs) sent
- Number of CCMs received
- Number of CCMs received out of sequence
- Number of CCMs received, but discarded due to the **maximum-meps** limit
- Number of loopback messages (LBMs), used for CFM ping
- Number of loopback replies (LBRs), used for CFM ping, sent and received
- Number of LBRs received out of sequence
- Number of LBRs received with bad data (such as LBRs containing padding which does not match the padding sent in the corresponding LBM)
- Number of alarm indication signal (AIS) messages sent and received
- Number of lock (LCK) messages received

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear counters for all MEPs:

```
RP/0/RP0:hostname# clear ethernet cfm local meps all
```

clear ethernet cfm peer meps

To clear all peer MEPs or peer MEPs for a specified local MEP, use the **clear ethernet cfm peer meps** command in EXEC mode.

clear ethernet cfm peer meps {**all** | **domain** *domain-name* {**all** | **service** *service-name* {**all** | **local mep-id** *id*}} | **interface** *interface-name* {**all** | **domain** *domain-name*}}

all	Clears counters for all peer MEPs.
domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance end points belong.
local mep-id *id*	Local maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *interface-name*	String of a maximum of 80 characters that identifies the Ethernet interface.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command removes all received CCMs and corresponding peer MEPs from the database (other than those configured with cross-check). The peer MEPs will be added again when the next CCM is received.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all peer MEPs:

```
RP/0/RP0:hostname# clear ethernet cfm peer meps all
```

clear ethernet cfm traceroute-cache

To remove the contents of the traceroute cache, use the **clear ethernet cfm traceroute-cache** command in EXEC mode.

clear ethernet cfm traceroute-cache {**all** | **domain** *domain-name* {**all** | **service** *service-name* {**all** | **mep-id** *id*}} | **interface** *interface-name* {**all** | **domain** *domain-name*}}

Syntax Description

domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance end points belong.
mep-id *id*	Maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *interface-name*	String of a maximum of 80 characters that identifies the Ethernet interface.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear all ethernet cfm traceroute-cache:

```
RP/0/RP0:hostname# clear ethernet cfm traceroute-cache all
```

clear ethernet lmi interfaces

To clear Ethernet LMI statistics on one or all interfaces, use the **clear ethernet lmi interfaces** command in EXEC configuration mode.

clear ethernet lmi interfaces {*type interface-path-id* | **all**}

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Specifies clearing of LMI statistics for all Ethernet interfaces running the E-LMI protocol.

Command Default

None

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operation
ethernet-services	execute

The following example shows how to clear E-LMI statistics for Gigabit Ethernet interface 0/0/0/0:

```
RP/0/RP0:hostname# clear ethernet lmi interfaces TenGigE0/0/0/0
```

clear ethernet oam statistics

To clear the packet counters on Ethernet OAM interfaces, use the **clear ethernet oam statistics** command.

clear ethernet oam statistics [{**interface** *type interface-path-id* | **location** *node-id* **all**}]

Syntax Description

interface *type interface-path-id*	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	Clears the statistics for a specific node. For more information about the syntax for the router, use the question mark (**?**) online help function.
node-id	Path ID of the node.
all	Clears the statistics for all nodes on the router.

Command Default

No parameters clears the packet counters on all Ethernet OAM interfaces.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	execute

Examples

The following example shows how to clear the packet counters on a specific interface:

```
RP/0/RP0:hostname# clear ethernet oam statistics interface TenGigE0/1/5/1
```

clear ethernet sla statistics all

To delete the contents of buckets containing SLA statistics collected by all operations probes, including on-demand operations, use the **clear ethernet sla statistics all** command in EXEC mode.

clear ethernet sla statistics all [**current** | **history**]

Syntax Description

all	Clears statistics for all operations.
history	Clears statistics for buckets which were earlier filled for all operations.
current	Clears statistics for buckets currently being filled for all operations.

Command Default

When **current** or **history** are not used, all buckets (current, old, new, half empty, and full) for all operations (including on-demand operations) are cleared. This is equivalent to restarting the operation.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows hwot to use the **clear ethernet sla statistics all** command:

```
RP/0/RP0:router# clear ethernet sla statistics all
```

clear ethernet sla statistics on-demand

To delete the contents of buckets containing SLA statistics collected by on-demand probes, use the **clear ethernet sla statistics on-demand** command in EXEC mode.

clear ethernet sla statistics [**current** | **history**] **on-demand** { **all** | *id* } [**interface** *type R/S/I/P* **domain** [**all** | *domain_name*]] **target** [**all** | **mac address** *address* | **mep-id** *id* | **interface all** }

Syntax Description

current	(Optional) Clears statistics for all buckets currently being filled.
history	(Optional) Clears statistics for all full buckets.
on-demand all	Clears statistics for all on-demand operations.
on-demand *id*	Clears statistics for the on-demand operation of the specified number.
domain all	Clears statistics for on-demand operations for all domains.
domain *domain_name*	Clears statistics for on-demand operations for the specified domain.
target all	Clears statistics for on-demand operations targeted to all MEPs for the specified interface domain.
target mac address*address*	Clears statistics for on-demand operations targeted to the specified MAC address.
target mep-id	Clears statistcs for on-demand operations targeted to the specified MEP ID.
interface all	(Optional) Clears statistics for on-demand operations on all interfaces.

Command Default

When **current** or **history** are not used, all buckets for on-demand operations (current, old, new, half empty, and full) are cleared. This is equivalent to restarting the operation.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

When you clear a bucket for a currently running probe, the remaining statistics are still collected and stored in that bucket.

Task ID

Task ID	Operation
ethernet-services	execute

Example

This example shows how to use the **clear ethernet sla statistics on-demand** command:

```
RP/0/RP0:router# clear ethernet sla statistics on-demand all
```

connection timeout

To configure the timeout value for an Ethernet OAM session, use the **connection timeout** command in Ethernet OAM configuration mode.

connection timeout *seconds*

Syntax Description

seconds	Connection timeout period in number of lost periodic information OAMPDUs. The range is 2 to 30.

Command Default

The default value is 5.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If no packets are received from the OAM peer in the specified connection timeout period which is measured in number of lost periodic Information OAMPDUs, then the OAM session is brought down, and the negotiation phase starts again.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to configure the connection timeout value of an Ethernet OAM session:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# connection timeout 20
```

continuity-check archive hold-time

To configure the time limit for how long peer maintenance-end-points (MEPs) are held in the continuity-check database after they have timed out (no more CCMs are received), use the **continuity-check archive hold-time** command in CFM domain service configuration mode. To return to the default value, use the no form of this command.

continuity-check archive hold-time *minutes*
no continuity-check archive hold-time *minutes*

Syntax Description

minutes	Time limit (in minutes) that peer MEPs are held in the continuity-check database before they are cleared. Range is 1 to 65535.

Command Default

The default is 100.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Peer MEPs appear in **show ethernet cfm peer meps** command display output after they timeout (no more continuity check messages (CCMs) are received).

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the time limit for how long continuity-check messages are held in the continuity-check archive:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# continuity-check archive hold-time 100
```

continuity-check interval

To enable continuity check and configure the time interval at which continuity-check messages are transmitted or to set the threshold limit for when a MEP is declared down, use the **continuity-check interval** command in CFM domain service configuration mode. To disable continuity check, use the **no** form of this command.

continuity-check interval *time* [**loss-threshold** *threshold*]
no continuity-check interval *time* [**loss-threshold** *threshold*]

Syntax Description

time	Interval at which continuity-check messages are transmitted. Valid values are: • 100ms: 100 milliseconds • 1s: 1 second • 10s: 10 seconds • 1m: 1 minute • 10m: 10 minutes
loss-threshold *threshold*	(Optional) Specifies the number of continuity-check messages that are lost before CFM declares that a MEP is down (unreachable). Range is 2 to 255. Used in conjunction with **interval**.

Command Default

Continuity check is off by default.

If **loss-threshold** is not specified, the default is 3.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to configure the time interval at which continuity-check messages are transmitted and set the threshold limit for when a MEP is declared down.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# continuity-check interval 100ms loss-threshold 10
```

continuity-check loss auto-traceroute

To configure automatic triggering of a traceroute when a MEP is declared down, use the **continuity-check loss auto-traceroute** command in CFM domain service configuration mode. To disable automatic triggering of a traceroute, use the no form of this command.

continuity-check loss auto-traceroute
no continuity-check loss auto-traceroute

This command has no keywords or arguments.

Command Default

Auto-trigger is off.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The results of the traceroute can be seen using the **show ethernet cfm traceroute-cache** command.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure automatic triggering of a traceroute when a MEP is declared down:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# continuity-check loss auto-traceroute
```

cos (CFM)

To configure the class of service (CoS) for all CFM packets generated by the maintenance end point (MEP) on an interface, use the **cos** command in interface CFM MEP configuration mode. To return to the default CoS, use the no form of this command.

cos *cos*
no cos *cos*

Syntax Description

cos	Class of Service for this MEP. The range is 0 to 7.

Command Default

When not configured, the default CoS value is inherited from the Ethernet interface.

Command Modes

Interface CFM MEP configuration (config-if-cfm-mep)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Configuring the class of service (CoS) on maintenance end points (MEPs) is supported on all Ethernet interfaces.

The specifed CoS value is used for all CFM messages transmitted by the MEP, except for the following:

- Loopback and Linktrace replies—These are transmitted using the CoS value received in the corresponding loopback or linktrace message.
- AIS messages—If a different CoS value is specified in the AIS configuration.

Note For Ethernet interfaces, the CoS is carried as a field in the VLAN tag. Therefore, CoS only applies to interfaces where packets are sent with VLAN tags. If the **cos (CFM)** command is specified for a MEP on an interface that does not have a VLAN encapsulation configured, an error message will be logged and no CFM packets will be sent.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the class of service (CoS) for a maintenance end point (MEP) on an interface.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/1
RP/0/RP0:hostname(config-if)# ethernet cfm mep domain Dm1 service Sv1 mep-id 1
RP/0/RP0:hostname(config-if-cfm-mep)# cos 7
```

debug ethernet cfm packets

To log debug messages about CFM packets that are sent or received by the Ethernet connectivity fault management (CFM) process, use the **debug ethernet cfm packets** command in EXEC mode.

debug ethernet cfm packets [**domain** *domain-name* [**service** *service-name* [**mep-id** *mep-id*]]] [**interface** *type interface-path-id* [**domain** *domain-name*]] [**packet-type** {**ccm** | **linktrace** | **loopback**}] [**remote mac-address** *mac-address*] [**remote mep-id** *mep-id*] [{**sent** | **received**}] [{**brief** | **full** | **hexdump**}]
debug ethernet cfm packets [**domain** *domain-name* [**service** *service-name* [**mep-id** *mep-id*]]] [**interface** *type interface-path-id* [**domain** *domain-name*]] [**packet-type** {**ais** | **ccm** | **delay-measurement** | **linktrace** | **loopback**}] [**remote mac-address** *mac-address*] [**remote mep-id** *mep-id*] [{**sent** | **received**}] [{**brief** | **full** | **hexdump**}]

Syntax Description

domain *domain-name*	(Optional) Filters packets for display by the specified CFM maintenance domain, where *domain-name* is a string of up to 80 characters.
service *service-name*	(Optional) Filters packets for display by the specified service name, where *service-name* is a string of up to 80 characters.
mep-id *mep-id*	(Optional) Filters packets for display by the specified maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *type interface-path-id*	(Optional) Filters packets for display by the specified physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
packet-type	(Optional) Filters packets for display by the specified packet type. The following packet types are valid: • **ais** • **ccm** • **delay-measurement** • **linktrace** • loopback
remote mac-address *mac-address*	(Optional) Filters packets for display by the specified MAC address.
remote mep-id *mep-id*	(Optional) Filters packets for display by the remote MEP properties.
sent	(Optional) Displays only sent packets.
received	(Optional) Displays only received packets.
brief	(Optional) Displays brief information about each packet.

full	(Optional) Displays a full decode of each packet.
hexdump	(Optional) Displays a full decode and hexadecimal output of each packet.

Command Default

If no parameters are specified, all CFM packets are debugged and logged.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Caution Enabling packet debugging without filters can have an adverse effect on the performance of the router. To avoid this, filters should always be specified to restrict the output to the domain, service, local MEP, interface, direction and packet type of interest.

Packets can be filtered for debugging by specifying any of the optional parameters.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows a sample output of the **debug ethernet cfm packets** command with a full decode and hexadecimal output for sent and received CCM packets:

```
RP/0/RP0:hostname# debug ethernet cfm packets hexdump

RP/0/RP0:hostname:May 29 14:15:39.621 : cfmd[150]: PKT-RX: TenGigE0/1/0/0 ingress: CCM
packet rcvd at level 2 for domain foo, service foo: length 91, src MAC 0001.0203.0402, dst
 MAC 0180.c200.0032: Packet processed successfully
RP/0/RP0:hostname:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Level 2, opcode CCM,
version 0, RDI bit unset, interval 10s, seq. num 1, remote MEP ID 16, flags 0x05, first TLV
 offset 70, 0 unknown TLVs
RP/0/RP0:hostname:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: MAID: MDID String 'dom4',
 SMAN String 'ser4'
RP/0/RP0:hostname:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Sender ID: Chassis ID
Local 'hpr', Mgmt Addr <none>
RP/0/RP0:hostname:May 29 14:15:39.621 : cfmd[150]: PKT-RX:   CCM: Port status: Up, interface
 status Up
RP/0/RP0:hostname:May 29 14:15:39.622 : cfmd[150]: PKT-RX:   Raw Frame:
RP/0/RP0:hostname:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x40010546 00000001 00100404
 646F6D34 02047365 72340000 00000000 00000000
RP/0/RP0:hostname:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x00000000 00000000 00000000
 00000000 00000000 00000000 00000000 00000000
RP/0/RP0:hostname:May 29 14:15:39.622 : cfmd[150]: PKT-RX:     0x00000000 00000000 00000200
 01020400 01010100 05030768 707200
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX: TenGigE0/1/0/0 egress: CCM packet
 sent at level 2 for domain foo, service foo: length 91, src MAC 0001.0203.0400, dst MAC
0180.c200.0032
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Level 2, opcode CCM,
version 0, RDI bit set, interval 10s, seq. num 16, remote MEP ID 1, flags 0x85, first TLV
```

```
offset 70, 0 unknown TLVs
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: MAID: MDID String 'foo',
 SMAN String 'foo'
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Sender ID: Chassis ID
Local 'ios', Mgmt Addr <none>
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   CCM: Port status: Up, interface
 status Up
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:   Raw Frame:
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x40018546 00000010 00010403
 666F6F02 03666F6F 00000000 00000000 00000000
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x00000000 00000000 00000000
 00000000 00000000 00000000 00000000 00000000
RP/0/RP0:hostname:May 29 14:15:43.625 : cfmd[150]: PKT-TX:     0x00000000 00000000 00000200
 01020400 01010100 05030769 6F7300
```

debug ethernet cfm protocol-state

To log debug messages about CFM state machines and protocol events, use the **debug ethernet cfm protocol-state** command in EXEC mode.

debug ethernet cfm protocol-state [**domain** *domain-name* [**service** *service-name* [**mep-id** *mep-id*]]] [**interface** *type interface-path-id* [**domain** *domain-name*]]

Syntax Description

domain *domain-name*	(Optional) Filters information for display by the specified CFM maintenance domain, where *domain-name* is a string of up to 80 characters.
service *service-name*	(Optional) Filters information for display by the specified service name, where *service-name* is a string of up to 80 characters.
mep-id *mep-id*	(Optional) Filters information for display by the specified maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *type interface-path-id*	(Optional) Filters information for display by the specified physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

If no parameters are specified, all CFM state machines and protocol events are debugged and logged.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Debug messages can be filtered by specifying any of the optional parameters.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows a sample output of the **debug ethernet cfm protocol-state** command.

```
RP/0/RP0:hostname# debug ethernet cfm protocol-state

RP/0/RP0:hostname:May 29 14:41:49.966 : cfmd[150]: CFM: Created 1 local MEPs in PM and
Engine
RP/0/RP0:hostname:May 29 14:41:49.967 : cfmd[150]: CFM: State changes notification for 1
EFPs
RP/0/RP0:hostname:May 29 14:42:14.143 : cfmd[150]: CFM: New remote MEP detected in domain
```

```
foo, service foo for local MEP ID 1 on interface TenGigE0/1/0/0; remote MEP ID 16, MAC
0001.0203.0402, errors: set: mismatched MAID; current: mismatched MAID;
RP/0/RP0:hostname:May 29 14:42:16.644 : cfmd[150]: CFM: Fault alarm notification for local
 MEP - domain: foo, service: foo, MEP ID: 1, interface: TenGigE0/1/0/0, defect: cross-connect
 CCM
RP/0/RP0:hostname:May 29 14:43:32.247 : cfmd[150]: CFM: Initiated exploratory linktrace to
 ffff.ffff.ffff from MEP in domain foo, service foo, MEP ID 1, interface TenGigE0/1/0/0
with ttl 64 and transaction ID 65537, reply-filtering Default and directed MAC None
May 29 14:43:49.155 : cfmd[150]: CFM: Remote MEP timed out in domain foo, service foo for
local MEP ID 1 on interface TenGigE0/1/0/0; remote MEP ID 16, MAC 0001.0203.0402, errors:
cleared: mismatched MAID; current: none
```

domain

To create and name a container for all domain configurations and enter the CFM domain configuration mode, use the **domain** command in CFM configuration mode. To remove the domain, use the no form of this command.

domain *domain-name* **level** *level-value* [**id null** [**dns** *dns-name*][**mac** *H.H.H*][**string** *string*]]
no domain *domain-name* **level** *level-value* [**id null** [**dns** *dns-name*][**mac** *H.H.H*][**string** *string*]]

Syntax Description

domain-name	Administrative name unique to this container, case sensitive ASCII string, up to 80 characters.
level *level-value*	The CFM protocol level of this domain. Range is 0 to 7.
id	(Optional) Maintenance domain identifier (MDID) used in conjunction with one of the following keywords to specify the MDID type and value: • null • **dns** *DNS-name* • **mac** *H.H.H* • **string** *string*
null	(Optional) Null value ID, used with the **id** keyword.
dns *DNS-name*	(Optional) DNS name, up to 43 characters in length, used with the **id** keyword.
mac *H.H.H*	(Optional) Hexadecimal MAC address, used with the **id** keyword.
string *string*	(Optional) Maintenance domain identifier (MDID) value, up to 43 characters in length, used with the **id** keyword. **Note** The domain name may be the used here as the maintenance domain identifier (MDID) if desired.

Command Default

If **id** is not specified, the domain name is used as the MDID.

Command Modes

CFM configuration (config-cfm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The level must be specified.

The maintenance domain identifier (MDID) is used as the first part of the maintenance association identifier (MAID) in CFM frames. If the MDID is not specified, the domain name is used as the MDID by default.

Multiple domains may be specified at the same level. If the MDID is specified as NULL, the MAID is constructed as a short maintenance association name.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to create a domain and give it a domain name, level, and maintenance domain identifier (MDID):

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)#
```

efd

To enable Ethernet Fault Detection (EFD) on all down Maintenance End Points (MEPs) in a down MEPs service, use the **efd** command in CFM domain service configuration mode. To disable EFD, use the no form of this command.

efd {**protection-switching**}
no efd

Syntax Description

protection-switching	Enables protection switching, which causes high-priority notifications to be sent when peer MEPs specified for cross-check time out, or when CCMs are received with the RDI bit set.

Note The high-priority notifications only apply to MEPs that are offloaded. In the case of non-offloaded MEPs, enabling protection switching has no effect, and the command only enables EFD.

Command Default

EFD is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

EFD can only be enabled for down MEPs within a down MEPs service.

If the **efd** command is issued when any MEP in the service has any of the following error conditions, the MEP will shut down the interface:

- The MEP appears cross-connected to another MAID.
- The MEP is receiving invalid CCMs, such as receiving its own MAC or MEP-ID.
- All peer MEPs are reporting a state other than UP via the Port Status TLV.
- A peer MEP is reporting a state other than UP in Interface Status TLV.
- When cross-check is configured, and a session with an expected MEP times out, EFD is triggered on the local MEP.
- No CCMs are received from a peer MEP appearing in the configured cross-check list.
- An RDI is being received from a peer MEP.
- The MEP is receiving an AIS/LCK.

The MEP will bring the interface back up when the error condition is no longer detected.

Note When an interface is shut down by a MEP using EFD, the MEP will continue to send and receive CCMs and other CFM messages.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to enable EFD:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain D1 level 1
RP/0/RP0:hostname(config-cfm-dmn)# service S1 down-meps
RP/0/RP0:hostname(config-cfm-dmn-svc)# efd
```

ethernet cfm (global)

To enter Connectivity Fault Management (CFM) configuration mode, use the **ethernet cfm (global)** command in global configuration mode.

ethernet cfm

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter the CFM configuration mode.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)#
```

ethernet cfm (interface)

To enter interface CFM configuration mode, use the **ethernet cfm (interface)** command in interface configuration mode.

ethernet cfm

Syntax Description

This command has no keywords or arguments.

Command Default

No MEPs are configured on the interface.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter interface CFM configuration mode:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/1
RP/0/RP0:hostname(config-if)# ethernet cfm
RP/0/RP0:hostname(config-if-cfm)#
```

ethernet lmi

To enable Ethernet Local Managment Interface (E-LMI) operation on an interface and enter interface Ethernet LMI configuration mode, use the **ethernet lmi** command in interface configuration mode. To disable Ethernet LMI and return to the default, use the **no** form of the command.

ethernet lmi
no ethernet lmi

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet LMI is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Ethernet LMI is supported only on physical Ethernet interfaces.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to enable Ethernet LMI on a Ten Gigabit Ethernet interface and enter Ethernet LMI configuration mode:

```
RP/0/RP0:hostname# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if-elmi)#
```

ethernet oam

To enable Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode, use the **ethernet oam** command in interface configuration mode. To disable Ethernet Link OAM, use the **no** form of this command.

ethernet oam
no ethernet oam

Syntax Description

This command has no keywords or arguments.

Command Default

When enabled on an interface, the Ethernet Link OAM default values apply.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When you enable Ethernet Link OAM on an interface, the default Ethernet Link OAM values are applied to the interface. For the default Ethernet Link OAM values, see the related Ethernet Link OAM commands.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable Ethernet Link OAM and enter interface Ethernet OAM configuration mode.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/5/6
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)#
```

ethernet sla

To enter the Ethernet Service Level Agreement (SLA) configuration mode, use the **ethernet sla** command in Global Configuration mode.

ethernet sla

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global Configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to you the **ethernet sla** command:

```
RP/0/RP0:router(config)# ethernet sla
```

ethernet oam profile

To create an Ethernet Operations, Administration and Maintenance (EOAM) profile and enter EOAM configuration mode, use the **ethernet oam profile** command. To delete an EOAM profile, use the **no** form of this command.

ethernet oam profile *profile-name*
no ethernet oam profile *profile-name*

Syntax Description

profile-name	Text string name of the OAM profile. The maximum length is 32 bytes.

Command Default

No default behavior or values

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Before you can delete an EOAM profile, you must remove the profile from all interfaces to which it is attached.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to create an Ethernet OAM profile and enter Ethernet OAM configuration mode:

```
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)#
```

ethernet uni id

To specify a name for the Ethernet User-Network Interface (UNI) link, use the **ethernet uni id** command in interface configuration mode.

ethernet uni id *name*

Syntax Description

name	Maximum of 64 characters to identify the Ethernet UNI link.

Command Default

No name is specified for the Ethernet UNI link.

Command Modes

Interface (config-if)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The UNI name should be unique among all UNIs that are part of a given Ethernet Virtual Connection (EVC).

When the Ethernet Local Management Interface (E-LMI) protocol is running on the UNI, the name specified in the **ethernet uni id** command is advertised by E-LMI to the Customer Edge (CE) device. It is also carried in Ethernet Connectivity Fault Management (CFM) Continuity Check Messages (CCMs) if there is an Up MEP on the UNI, and passed to E-LMI on the peer MEP so that it can be advertised to the remote CE device.

Task ID

Task ID	Operation
interface	read, write

The following example shows how to configure the UNI name called "PE1-CustA-Slot0-Port0" on Ten Gigabit Ethernet interface 0/0/0/0:

```
RP/0/RP0:hostname(config)# interface TenGigE0/0/0/0
RP/0/RP0:hostname(config-if)# ethernet uni id PE1-CustA-Slot0-Port0
```

extension remote-uni disable

To disable transmission of the Cisco-proprietary Remote UNI Details information element in Ethernet LMI (E-LMI) STATUS messages, use the **extension remote-uni disable** command in interface Ethernet LMI configuration mode. To return to the default, use the **no** form of the command.

extension remote-uni disable
no extension remote-uni disable

This command has no keywords or arguments.

Command Default

The Cisco-proprietary Remote UNI Details information element is sent in E-LMI STATUS messages.

Command Modes

Interface Ethernet LMI configuration (config-if-elmi)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **extension remote-uni disable** command to have stricter conformance to the MEF 16 E-LMI specification for information elements in STATUS messages.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to disable transmission of the Cisco-proprietary Remote UNI Details information element:

```
RP/0/RP0:hostname# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if-elmi)# extension remote-uni disable
```

frame-seconds threshold

To configure the thresholds that trigger a frame-seconds error event, use the **frame-seconds threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame-seconds threshold low *threshold* [**high** *threshold*]
no frame-seconds threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in seconds, that triggers a frame-seconds error event. The range is 0 to 900.
high *threshold*	(Optional) High threshold, in seconds, that triggers a frame-seconds error event. The range is 1 to 900. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default value is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When the low threshold is passed, a frame-seconds error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the low and high thresholds that trigger a frame-seconds error event:

```
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# link-monitor
RP/0/RP0:hostname(config-eoam-lm)# frame-seconds threshold low 10 high 900
```

frame-seconds window

To configure the window size for the OAM frame-seconds error event, use the **frame-seconds window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame-seconds window *window*
no frame-seconds window *window*

Syntax Description

window	Size of the window for a frame-seconds error in milliseconds. The range is 10000 to 900000.

Command Default

The default value is 60000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the window size for a frame-seconds error.

```
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# link-monitor
RP/0/RP0:hostname(config-eoam-lm)# frame-seconds window 900000
```

frame threshold

To configure the thresholds that triggers an Ethernet OAM frame error event, use the **frame threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the threshold to the default value, use the **no** form of this command.

frame threshold low *threshold* [**high** *threshold*]
no frame threshold low *threshold* [**high** *threshold*]

Syntax Description

low *threshold*	Low threshold, in symbols, that triggers a frame error event. The range is 0 to 12000000.
high *threshold*	(Optional) High threshold, in symbols, that triggers a frame error event. The range is 0 range is 0 to 12000000. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default

The default low threshold is 1.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When the low threshold is passed, a frame error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the low and high thresholds that trigger a frame error event:

```
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# link-monitor
RP/0/RP0:hostname(config-eoam-lm)# frame threshold low 100 high 60000
```

frame window

To configure the frame window size of an OAM frame error event, use the **frame window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To return the window size to the default value, use the **no** form of this command.

frame window *window*
no frame window *window*

Syntax Description

window	Size of the window for a frame error in seconds. The range is 1000 to 60000.

Command Default

The default value is 1000.

Command Modes

Ethernet OAM link monitor configuration (config-eoam-lm)

Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the window size for a frame error.

```
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# link-monitor
RP/0/RP0:hostname(config-eoam-lm)# frame window 60
```

hello-interval

To specify the time interval between hello packets for an Ethernet OAM session, use the **hello-interval** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of the command.

hello-interval {**100ms** | **1s**}
no hello-interval {**100ms** | **1s**}

Syntax Description

100ms	Specifies a 100-millisecond interval between hello packets.
1s	(Interface Ethernet OAM configuration mode only) Specifies a 1-second interval between hello packets. This is the default.

Command Default

The default is 1 second.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If a profile exists on the interface, setting the mode with this command overrides the mode setting in the profile on an interface.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to set the hello interval to 100 milliseconds on a Gigabit Ethernet interface:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/5/6
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# profile Profile_1
RP/0/RP0:hostname(config-if-eoam)# hello-interval 100ms
```

log ais

To configure AIS logging for a Connectivity Fault Management (CFM) domain service to indicate when AIS or LCK packets are received, use the **log ais** command in CFM domain service configuration mode. To disable AIS logging, use the no form of this command.

log ais
no log ais

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure AIS logging for a Connectivity Fault Management (CFM) domain service to indicate when AIS or LCK packets are received:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain D1 level 1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# log ais
```

log continuity-check errors

To enable logging of continuity-check errors, use the **log continuity-check errors** command in CFM domain service configuration mode. To disable logging of continuity-check errors, use the no form of this command.

log continuity-check errors
no log continuity-check errors

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The following types of continuity-check errors are logged:

- Incorrect level (cross-connect)
- Incorrect interval
- Incorrect MA-ID (cross-connect)
- Local MAC address received (loop)
- Local MEP-ID received (mis-config)
- Invalid source MAC received
- RDI received

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable logging of continuity check errors:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# log continuity-check errors
```

log continuity-check mep changes

To enable logging of peer maintenance-end-point (MEP) state changes, use the **log continuity-check mep changes** command in CFM domain service configuration mode. To disable logging of peer MEP state changes, use the no form of this command.

log continuity-check mep changes
no log continuity-check mep changes

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command enables logging of state changes that occur in MEPs for a particular service, such as:

- New peer MEP detected.
- Peer MEP time out (loss of continuity) detected.

Note If a Local MEP is receiving Wrong Level CCMs, then a transient timeout might occur when correct Level CCMs are received again.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable logging of continuity-check mep changes:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# log continuity-check mep changes
```

log crosscheck errors

To enable logging of crosscheck error events, use the **log crosscheck errors** command in CFM domain service configuration mode. To disable logging of crosscheck error events, use the no form of this command.

log crosscheck errors
no log crosscheck errors

Syntax Description

This command has no keywords or arguments.

Command Default

Logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command enables logging of crosscheck errors, such as:

- MEPs missing
- Additional peer MEPs detected

Note Crosscheck errors are only detected and logged when crosscheck is configured using the **mep crosscheck** and **mep-id** commands.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable logging of crosscheck errors:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# log crosscheck errors
```

log disable

To turn off syslog messages for Ethernet LMI (E-LMI) errors or events, use the **log disable** command in interface Ethernet LMI configuration mode. To return to the default, use the **no** form of the command.

log {**errors** | **events**} **disable**
no log {**errors** | **events**} **disable**

Syntax Description

errors	Disables logging of E-LMI protocol and reliability errors.
events	Disables logging of significant E-LMI protocol events.

Command Default

E-LMI syslog messages are enabled for errors and events.

Command Modes

Interface Ethernet LMI configuration (config-if-elmi)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To see statistics on E-LMI protocol and reliability errors and protocol events, use the **show ethernet lmi interfaces** command.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to disable logging of E-LMI protocol and reliability errors:

```
RP/0/RP0:hostname# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if-elmi)# log errors disable
```

The following example shows how to disable logging of E-LMI events:

```
RP/0/RP0:hostname# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if-elmi)# log events disable
```

log efd

To enable logging of Ethernet Fault Detection (EFD) state changes to an interface (such as when an interface is shut down or brought up via EFD), use the **log efd** command in CFM domain service configuration mode. To disable EFD logging, use the no form of this command.

log efd
no log efd

Syntax Description

This command has no keywords or arguments.

Command Default

EFD logging is disabled.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When EFD logging is enabled, a syslog is generated whenever the EFD state of an interface changes.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable EFD logging:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain D1 level 1
RP/0/RP0:hostname(config-cfm-dmn)# service S1 down-meps
RP/0/RP0:hostname(config-cfm-dmn-svc)# log efd
```

maximum-meps

To configure the maximum number of maintenance end points (MEPs) for a service, use the **maximum-meps** command in CFM domain service configuration mode. To return to the default value, use the no form of this command.

maximum-meps *number*

Syntax Description

number	Maximum number of MEPs allowed for this service. The range is 2 to 8190.

Command Default

The default is 100.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command configures the maximum number of peer maintenance end points (MEPs). It does not limit the number of local MEPs. The configured **maximum-meps** *number* must be at least as great as the number of configured crosscheck MEPs.

The **maximum-meps** *number* limits the number of peer MEPs, for which local MEPs store continuity-check messages (CCMs). When the limit is reached, CCMs from any new peer MEPs are ignored, but CCMs from existing peer MEPs continue to be processed normally.

The **maximum-meps** *number* also limits the size of the CCM learning database.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to configure the maximum number of maintenance end points (MEPs) for a service:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# maximum-meps 4000
```

mep crosscheck

To enter CFM MEP crosscheck configuration mode, use the **mep crosscheck** command in CFM domain service configuration mode.

mep crosscheck

Syntax Description

This command has no keywords or arguments.

Command Default

Not configured, in which case no crosscheck is performed on the MEP.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enter CFM MEP crosscheck configuration mode:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# mep crosscheck
RP/0/RP0:hostname(config-cfm-xcheck)#
```

mep-id

To enable crosscheck on a maintenance end point (MEP), use the **mep-id** command in CFM MEP crosscheck configuration mode. To disable crosscheck on a MEP, use the **no** form of this command.

mep-id *mep-id-number* [**mac-address** *mac-address*]
no mep-id *mep-id-number* [**mac-address** *mac-address*]

Syntax Description

mac *mac-address*	(Optional) MAC address of the interface upon which the MEP resides, in standard hexadecimal format, hh:hh:hh:hh:hh:hh.

Command Default

Not configured, in which case no crosscheck is performed on the MEP.

Command Modes

CFM MEP crosscheck configuration (config-cfm-xcheck)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command enables Crosscheck on the maintenance end point (MEP) specified by the MEP ID number (*mep-id-number*). The range for MEP ID numbers is 1 to 8191. Crosscheck is enabled when the first crosscheck MEP is entered.

Repeat this command for every MEP that you want to include in the expected set of MEPs for crosscheck.

Crosscheck detects the following two additional defects for continuity-check messages (CCMs) on peer MEPs:

- Peer MEP missing—A crosscheck MEP is configured, but has no corresponding peer MEP from which to receive CCMs.
- Peer MEP unexpected—A peer MEP is sending CCMs, but no crosscheck MEP is configured for it.

Note If more than one local MEP is configured for a service, all the local MEPs must be included in the list of configured crosscheck MEPs.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to statically define a maintenance end point (MEP) under a service, so that it can be crosschecked.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# mep crosscheck
```

```
RP/0/RP0:hostname(config-cfm-xcheck)# mep-id 10
```

mep domain

To create a maintenance end point (MEP) on an interface, use the **mep domain** command in interface CFM configuration mode. To remove the MEP from the interface, use the **no** form of this command.

mep domain *domain-name* **service** *service-name* **mep-id** *id-number*
no mep domain *domain-name* **service** *service-name* **mep-id** *id-number*

Syntax Description

domain *domain-name*	Domain in which to create the maintenance end point (MEP).
service *service-name*	Operation service in which to create the maintenance end point (MEP).
mep-id *id-number*	Maintenance end points (MEP) identifier to assign to this MEP. The range is 1 to 8191.

Command Default

No MEPs are configured on the interface.

Command Modes

Interface CFM configuration (config-if-cfm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

CFM Maintenance end points (MEPs) are supported on all Ethernet interfaces and VLAN subinterfaces.

This command creates MEPs in the UP MEP state, unless the specified **service** is configured with MEPs in the DOWN MEP state.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to create a MEP using an ID of 1 on the CFM domain named DM1 and service named Sv1:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/1
RP/0/RP0:hostname(config-if)# ethernet cfm
RP/0/RP0:hostname(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
```

mib-retrieval

To enable MIB retrieval in an Ethernet OAM profile or on an Ethernet OAM interface, use the **mib-retrieval** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return the interface to the default (disabled), use the **disable** keyword.

mib-retrieval [**disable**]

Syntax Description

disable	Disables MIB retrieval the Ethernet OAM interface.

Command Default

MIB retrieval is disabled by default.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When MIB retrieval is enabled on an Ethernet OAM interface, the OAM client advertises support for MIB retrieval to the peer.

When MIB retrieval is disabled (the default), only the enable form of the **mib-retrieval** command is available in interface Ethernet OAM configuration mode. The **disable** keyword is provided to override the profile when needed.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable MIB retrieval on a Gigabit Ethernet interface:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/5/6
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# mib-retrieval
```

mip auto-create

To enable the automatic creation of Maintenance Intermediate Points (MIPs) in a cross-connect, use the **mip auto-create** command in CFM domain service configuration mode. To disable automatic creation of MIPs, use the **no** form of this command.

mip auto-create {**all** | **lower-mep-only**}{}
no mip auto-create {**all** | **lower-mep-only**}

Syntax Description

all	Enables automatic creation of MIPs on all interfaces.
lower-mep-only	[Optional] Enables automatic creation of MIPs only on interfaces with a MEP at a lower level.

Command Default

None

Command Modes

CFM domain service configuration (config-cfm-dmn-svc) mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The MIP auto-creation feature is configured only for services associated with cross-connects.

Unlike MEPs, MIPs are not explicitly configured on each interface. MIPs are created automatically according to the algorithm specified in the CFM 802.1ag standard. For each interface, the algorithm, in brief, operates in this manner:

- The cross-connect for the interface is found, and all services associated with that cross-connect are considered for MIP auto-creation.
- The level of the highest-level MEP on the interface is found. From among the services considered above, the service in the domain with the lowest level that is higher than the highest MEP level is selected. If there are no MEPs on the interface, the service in the domain with the lowest level is selected.
- The MIP auto-creation configuration for the selected service is examined to determine whether a MIP should be created.

Note Configuring a MIP auto-creation policy for a service does not guarantee that a MIP will automatically be created for that service. The policy is only considered if that service is first selected by the algorithm.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

This example shows how to enable the automatic creation of MIPs for all interfaces in a cross connect:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# mip auto-create all
```

mode (Ethernet OAM)

To configure the Ethernet OAM mode on an interface, use the **mode** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of the command.

mode {**active** | **passive**}

Syntax Description

passive	Specifies that the interface operates in passive mode, where it cannot initiate the discovery process, generate a retrieval PDU.
active	(Interface Ethernet OAM configuration only) Specifies that the interface operates in active mode to initiate processes and make requests.

Command Default

The default is active.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If a profile exists on the interface, setting the mode with this command overrides the mode setting in the profile on an interface.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable Ethernet OAM passive mode on a Ten Gigabit Ethernet interface:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/5/6
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# profile Profile_1
RP/0/RP0:hostname(config-if-eoam)# mode passive
```

packet size

To configure the minimum size (in bytes) for outgoing probe packets, including padding when necessary, use the **packet size** command in SLA profile probe configuration mode.

packet size *bytes*

Syntax Description

bytes	Minimum size of the packet including padding when necessary. The range is 1 to 9000 bytes. This value refers to the total frame size including the Layer 2 or Layer 3 packet header.

Command Default

The minimum packet size is not configured. When a minimum packet size is configured and padding is required, the default padding is all 0s.

Command Modes

SLA profile probe configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

For supported packet types, this configuration determines the minimum size of all outgoing SLA probe packets, including the size to which they are padded. The amount of padding that is added to a packet depends on the type of frame that is sent and the amount of data in the frame.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **packet size** command:

```
RP/0/RP0:router(config-sla-prof-pb)# packet size 9000
```

priority

To configure the priority of outgoing SLA probe packets, use the **priority** command in SLA profile probe configuration mode.

priority *priority_level*

Syntax Description

priority_level	Priority level. The range is 0 to 7.

Command Default

No default behavior or values.

Command Modes

SLA profile probe configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

The default priority for all CFM operation types is the Class of Service (CoS) priority for the egress interface. SLA operations that are configured on Maintenance End Points (MEPs) do not use the Class of Service (CoS) settings that are configured independently on Maintenance End Points (MEPs). Use this command to change the priority level of SLA probe packets.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **priority** command:

```
RP/0/RP0:router(config-sla-prof-pb)# priority 7
```

probe

To enter SLA profile probe configuration mode, use the **probe** command in SLA profile configuration mode.

probe

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values.

Command Modes SLA profile configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines Each profile may optionally have 1 probe submode.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **probe** command:

```
RP/0/RP0:router(config-sla-prof)# probe
```

ping ethernet cfm

To send Ethernet connectivity fault management (CFM) loopback messages to a maintenance end point (MEP) or MAC address destination from the specified source MEP, and display a summary of the responses, use the **ping ethernet cfm** command in EXEC mode.

ping ethernet cfm domain *domain-name* **service** *service-name* {**mac-address** *mac* | **mep-id** *id*} **source** [**mep-id** *source-id*] **interface** *interface-path-id* [**cos** *cos-val*] [**count** *n*] [**frame-size** *size*] [**data-pattern** *hex*] [**interval** *seconds*] [**timeout** *time*]

Syntax Description

domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the maintenance points reside. **Note** For more information about the syntax, use the question mark (**?**) online help function.
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
mac-address *mac*	6-byte ID number of the MAC address of the destination MEP.
mep-id *id*	Maintenance end point (MEP) ID number of the destination MEP. The range for MEP ID numbers is 1 to 8191.
source	Source information.
mep-id *source-id*	(Optional) Maintenance end point (MEP) ID number of the source MEP. The range for MEP ID numbers is 1 to 8191.
interface *interface-path-id*	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
cos *cos-val*	(Optional) Class of Service (CoS) value that identifies the class of traffic of the source MEP. The valid values are from 0 to 7.
count *n*	(Optional) Number of pings as an integer value. The default is 5.
frame-size *size*	(Optional) Size, as an integer, of the ping frames. Frames are padded to read the specified size. The default is 0 (no padding)
data-pattern *hex*	(Optional) Hexadecimal value to be used as the data pattern for padding within a ping frame, when padding is required due to the **frame-size** configuration. The default is 0.
interval *seconds*	(Optional) Specifies, in seconds, the time between pings. The *n* argument is entered in seconds. The default is 1 second.

timeout *time*	(Optional) Timeout, in seconds, for the ping packet. The default is 2.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Before you can use this command, a local MEP must be configured for the domain and the interface.

The command displays the following infomation:

- Number of loopback message being sent
- Timeout period
- Domain name
- Domain level
- Service name
- Source MEP ID
- Interface
- Target MAC address
- MEP ID – If no MEP ID is specified, “No MEP ID specified” is displayed.
- Running time for the current ping operation to complete

Note The remaining information is not displayed until the current ping operation is complete. If the user interrupts the operation during this time (by pressing control-C), the prompt is returned and no further information is displayed. However, all loopback messages continue to be sent.

- Success rate of responses received – displayed as a percentage followed by the actual number of responses
- The round trip time minimum/maximum/average in milliseconds
- Out-of-sequence responses – displayed as a percentage followed by the actual number of out-of-sequence responses when at least one response is received. An out-of-sequence response occurs if the first response does not correspond with the first message sent, or a subsequent response is not the expected next response after a previously received response.
- Bad data responses – displayed as a percentage followed by the actual number of bad data responses when at least one response is received. A bad data response occurs if the padding data in the response does not match the padding data that in the sent message. This can only happen if the sent message is padded using the **frame-size** option.
- Received packet rate – displayed in packets per second when at least two responses are received. This approximate rate of response is the time between the first response received and the last response received, divided by the total number of responses received.

Task ID

Task ID	Operations
basic-services	execute
ethernet-services	execute

Examples

The following example shows how to send an Ethernet CFM loopback message:

```
RP/0/RP0:hostname# ping ethernet cfm domain D1 service S1 mep-id 16 source
interface TenGigE0/0/0/0

Type escape sequence to abort.
Sending 5 CFM Loopbacks, timeout is 2 seconds -
Domain foo (level 2), Service foo
Source: MEP ID 1, interface TenGigEt0/0/0/0
Target: 0001.0002.0003 (MEP ID 16):
  Running (5s) ...
Success rate is 60.0 percent (3/5), round-trip min/avg/max = 1251/1349/1402 ms
Out-of-sequence: 0.0 percent (0/3)
Bad data: 0.0 percent (0/3)
Received packet rate: 1.4 pps
```

polling-verification-timer

To set or disable the Metro Ethernet Forum (MEF) T392 Polling Verification Timer (PVT) for Ethernet Local Management Interface (E-LMI) operation, use the **polling-verification-timer** command in interface Ethernet LMI configuration mode. To return to the default, use the **no** form of the command.

polling-verification-timer {*interval* | **disable**}
no polling-verification-timer {*interval* | **disable**}

Syntax Description

interval	Number of seconds in the range 5 to 30. The default is 15.
disable	Turns off the timer.

Command Default

The T392 Polling Verification Timer is set to 15 seconds.

Command Modes

Interface Ethernet LMI configuration (config-if-elmi)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The PVT specifies the allowable time between transmission of a STATUS message and receipt of a STATUS ENQUIRY from the Customer Edge (CE) device before recording an error. If the PVT expiration time is reached on consecutive packets for the number of times specified by the **status-counter** command without a STATUS ENQUIRY being received, the E-LMI protocol status is changed to Down.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to set the MEF Polling Verification Timer for E-LMI to 30 seconds:

```
RP/0/RP0:hostname# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if-elmi)# polling-verification-timer 30
```

profile (EOAM)

To attach an Ethernet OAM profile to an interface, use the **profile** command in interface Ethernet OAM configuration mode. To remove the profile from the interface, use the no form of this command.

profile *name*
no profile *name*

Syntax Description

name	Text name of the Ethernet OAM profile to attach to the interface.

Command Default

No profile is attached.

Command Modes

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When an Ethernet OAM profile is attached to an interface using this command, all of the parameters configured for the profile are applied to the interface.

Individual parameters that are set by the profile configuration can be overridden by configuring them directly on the interface.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to attach an Ethernet OAM profile to a Ten Gigabit Ethernet interface.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/5/6
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# profile Profile_1
```

profile

To create an SLA operation profile and enter the SLA profile configuration mode, use the **profile** command in SLA configuration mode.

profile *profile_name* **type** { **cfm-delay-measurement** | **cfm-loopback** | **cfm-synthetic-loss-measurement** }

Syntax Description

profile_name	Profile name, case-sensitive string up to 31 characters in length. The name *all*cannot be used.
type	Specifies the type of packets sent by operations in this profile. Valid types are: • **cfm-delay-measurement** : CFM delay measurement packets • **cfm-loopback** : CFM loopback packets • **cfm-synthetic-loss-measurement** : CFM synthetic loss measurement packets

Command Default

No default behavior or values

Command Modes

Ethernet SLA configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

Each profile is uniquely identified by its name. Changing the packet **type** for the profile removes all stored data from the profile and is equivalent to deleting the profile and creating a new profile.

Note You can configure the Ethernet SLA profile to use Y.1731 DMM frames. The restriction of 150 configured Ethernet SLA operations for each CFM MEP is removed not only for profiles using DMM frames, but also for profiles using the other supported Y.1731 frame types, such as loopback measurement and synthetic loss measurement.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to configure an SLA operation profile and enter the SLA profile configuration mode:

```
RP/0/RP0:router(config-sla)# profile  p1  type  cfm-delay-measurement
```

require-remote

To require that certain features are enabled before an OAM session can become active, or to disable a requirement that is part of an active OAM profile, use the **require-remote** command in Ethernet OAM configuration or interface Ethernet OAM configuration mode. To remove the configuration and return to the default, use the **no** form of this command.

require-remote {**mode** {**active** | **passive**} | **mib-retrieval** | [**disabled**]}
no require-remote {**mode** {**active** | **passive**} | **mib-retrieval** | [**disabled**]}

Syntax Description

mode {**active** | **passive**}	Requires that active or passive mode is configured on the peer device before the OAM profile can become active.
mib-retrieval	Requires that MIB-retrieval is configured on the peer device before the OAM profile can become active.
disabled	(Optional—Interface Ethernet OAM configuration only) Overrides the Ethernet OAM profile configuration for this option and disables the feature at the specified interface.

Command Default

No default behavior or values

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **disabled** keyword is available only when you are configuring Ethernet OAM on an interface, and is used to override the configuration that is part of an active OAM profile.

The **disabled** keyword does not remove the configuration of the command. Use the **no** form of this command to do that.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to require that specific features are enabled before an OAM session can become active

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# require-remote mode active
RP/0/RP0:hostname(config-eoam)# require-remote mib-retrieval
```

The following example shows how to disable requirements on a particular interface that is part of an active OAM profile:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/6/5/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# require-remote mode active disabled
RP/0/RP0:hostname(config-if-eoam)# require-remote mib-retrieval disabled
```

schedule

To schedule an operation probe in a profile, use the **schedule** command in SLA profile configuration mode.

Hourly Scheduling

schedule every number { hours | minutes} { for duration { **seconds** | **minutes** | **hours** }

Daily Scheduling

schedule every day [at hh:mm] { for duration { **seconds** | **minutes** | **hours** | **days** }

Weekly Scheduling

schedule every week at hh:mm { for duration { **seconds** | **minutes** | **hours** | **days** | **week** }

Syntax Description

every number (hours | minutes}	Schedules a probe every specified number of hours or minutes , for the specified duration .
every day [at hh:mm]	Schedules a probe every day at the scheduled time for a specified duration.
every week at hh:mm	Schedules a probe one day per week, on the specified day , at the specified time (hh:mm), for the specified duration .
day	Day of the week.
hh:mm [ss]	Time of day in 24-hour format.
for duration	Duration of the probe. The valid values are: • 1 week • 1 day • 1 to 3600 seconds • 1 to 1440 minutes • 1 to 24 hours
number	Number of hours or minutes. The values are: • For hours, acceptable values are the factors of 24: 1, 2, 3, 4, 6, 8, 12 • For minutes, acceptable values are the factors of 1440 up to 90: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 30, 32, 36, 40, 45, 48, 60, 80, 90

Command Default

The default is every hour.

Command Modes

SLA profile configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

Schedules are optional, but a profile may contain only one schedule.

The **for** duration option must be specified if (and only if) the probe is configured to send multiple packets (or bursts of packets), using the **send packet every** or **send burst every** configuration of the **send (SLA)** command. If the **send (SLA)** command is not configured for the probe, or if **send burst once** is configured, the **for** duration option must not be used. If it is used in those cases, an error is returned.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **schedule** command for weekly scheduling:

```
RP/0/RP0:router(config-sla-prof)# schedule every week on Wednesday at 23:30 for 1 hour
```

send

To configure the number and timing of packets sent by a probe in an operations profile, use the **send** command in SLA profile probe configuration mode.

send { **burst** | **packet** } { **every** *number* { **seconds** | **minutes** | **hours** } } | **once** } **packet count** *packets* **interval** *number* { **seconds** | **milliseconds** }

Syntax Description

burst every *number*	Sends a burst of packets every specified number of seconds, minutes, or hours, where number is in the following range: • 1–3600 seconds • 1–1440 minutes • 1–168 hours
burst once	Sends a single burst one time.
packet count *packets*	Specifies the number of packets in each burst. The range is 2 to 600.
interval *number*	Specifies the time interval (in seconds or milliseconds) between each packet in a burst, where number is in the following range: • 1–30 seconds • 50–10000 milliseconds in multiples of 50 milliseconds
packet every *number*	Sends one packet every specified number of milliseconds, seconds, minutes, or hours, where number is in the following range: • 1–3600 seconds • 1–1440 minutes • 1–168 hours • 50–10000 milliseconds in multiples of 50 milliseconds
packet once	Sends a single packet one time.

Command Default

If the operation is configured to measure jitter or data packet loss, the default is to send a single burst of 2 packets with a second interval between the packets.

If the operation is configured to measure synthetic packet loss, the default is to send a single burst of 10 packets with a 100 millisecond interval between the packets.

If the operation does not calculate jitter, data, or synthetic packet loss, the default is to send a single packet one time.

Command Modes

SLA profile probe configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

The minimum **interval** supported is platform and packet-type dependent, so certain a configuration may cause an error even if it falls within the specified limits. In the case of Ethernet SLA, the shortest interval for packet types not used for synthetic loss measurement is 100ms.

When **burst once** is sent, a single burst is sent at the start of the probe. If the schedule defines a duration for the probe, a configuration warning is flagged. The same is true if the default is in effect.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **send** command:

```
RP/0/RP0:router(config-sla-prof-pb)# send burst every 60 seconds packet count 30 interval
1 second
```

statistics

To enable the collection of Ethernet Service Level Agreement (SLA) statistics, and enter the SLA profile statistics configuration mode, use the **statistics measure** command in SLA profile configuration mode.

statistics measure { **round-trip-delay** | **round-trip-jitter** }

Syntax Description

round-trip-delay	CFM delay measurement and CFM loopback profile types only) Enables the collection of statistics that measure the delay in the round trip of a packet.
round-trip-jitter	(CFM delay measurement and CFM loopback profile types only) Enables the collection of statistics that measure the amount of delay variance in the round trip of a packet.

Command Default

No statistics are collected

Command Modes

SLA profile configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

For statistics to be collected, at least one statistics entry must be present in each profile. To measure more than one type of statistic, this command may be configured more than once in a single profile.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

This example shows how to use the **statistics measure** command:

```
RP/0/RP0:router(config-sla-prof)# statistics measure round-trip-delay
```

service

To associate a service with a domain and enter CFM domain service configuration mode, use the **service** command in CFM domain configuration mode. To remove a service from a domain, use the **no** form of this command.

service *service-name* {**down-meps** | **xconnect group** *xconnect-group-name***p2p** *xconnect-name* | }} [{**id** [**icc-based** *icc-string umc-string*] | | [**string** *text*] | [**number** *number*] | [**vlan-id** *id-number*] | [**vpn-id** *oui-vpnid*]}]
no service *service-name* {**down-meps** | **xconnect group** *xconnect-group-name* **p2p** *xconnect-name* | }} [{**id** [**icc-based** *icc-string umc-string*] | | [**string** *text*] | [**number** *number*] | [**vlan-id** *id-number*] | [**vpn-id** *oui-vpnid*]}]

Syntax Description

service-name	Administrative name for the service. Case sensitive ASCII string up to 80 characters. Used in conjunction with one of the following service types: • **down-meps** • xconnect
down-meps	Specifies that all MEPs are down and no MIPs are permitted.
xconnect	Specifies the use of a cross connect. Used in conjunction with **group** and p2p. **Note** When **xconnect** is specified, all MEPs are up and MIPs are permitted.
group *xconnect-group-name*	Specifies the name of the cross connect group.
p2p *xconnect-name*	Specifies the name of the point-to-point cross connect and enters the Ethernet CFM domain service mode.
mp2mp *xconnect-name*	Specifies the name of the multipoint-to-multipoint cross connect and enters the Ethernet CFM domain service mode.
ce-id *ce-id-value*	Specifies the local Customer Edge (CE) identifier.
remote-ce-id *remote-ce-id-value*	Specifies the remote Customer Edge (CE) identifier.
id	(Optional) Service identifier. Valid service identifiers are: • **icc-based** *icc-string umc-string*—ITU-based Carrier Code format, with the total ICC and Unique MEG ID Code (UMC) string length no greater than 13 characters. • **number** *number*—Number from 0 to 65535.

Command Modes

CFM domain configuration (config-cfm-dmn)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The Short MA Name is the second part of the Maintenance Assoication Identifier (MAID) in CFM frames.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to specify that all MEPs are down and no MIPs are permitted, and enter CFM domain service configuration mode.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service Serv_1 down-meps
RP/0/RP0:hostname(config-cfm-dmn-svc)#
```

The following example shows how to associate a p2p cross connect service to a domain and enter CFM domain service configuration mode.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id string D1
RP/0/RP0:hostname(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p X1
RP/0/RP0:hostname(config-cfm-dmn-svc)#
```

show efd interface

To display all interfaces that are shut down because of Ethernet Fault Detection (EFD), or to display whether a specific interface is shut down because of EFD, use the **show efd interface** command.

show efd interface [*type interface-path-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If no parameters are specified, all interfaces that are shut down because of EFD are displayed.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If this command is issued when no EFD errors are detected, the system displays the following message:

```
< date time >
No matching interfaces with EFD-shutdown triggered
```

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to display all interfaces that are shut down because of Ethernet Fault Detection (EFD):

```
RP/0/RP0:hostname# show efd interfaces

Server VLAN MA
==============
Interface         Clients
------------------------
TenGigE0/0/0/0.0  CFM
```

show ethernet sla configuration-errors

To display information about errors that are preventing configured Ethernet Service Level Agreement (SLA) operations from becoming active, as well as any warnings that have occurred, use the **show ethernet sla configuration-errors** command in EXEC mode.

show ethernet sla configuration-errors [**domain** *domain_name*] [**interface** *type R/S/I/P*] [**profile** *profile_name*]

Syntax Description

domain *domain_name*	Displays information for the specified domain, where domain-name is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.
interface *type R/S/I/P*	Displays information for the specified interface.
profile *profile_name*	Displays information for the specified profile.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
ethernet-services	read

Example

This example shows how to use the **show ethernet sla configuration-errors** command:

```
RP/0/RP0:router# show ethernet sla configuration-errors
```

show ethernet sla operations

To display information about configured Ethernet Service Level Agreement (SLA) operations, use the **show ethernet sla operations** command in EXEC mode.

show ethernet sla operations [**detail**] [**domain** *domain_name*] [**interface** *type R/S/I/P* [**on-demand all**] [**profile** { *profile_name* | **all** }]

Syntax Description

detail	Displays detailed information.
domain *domain_name*	Displays information for the specified domain, where domain-name is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.
interface *type R/S/I/P*	Displays information for the specified interface.
profile *profile_name*	Displays information for the specified profile.
profile all	Displays information for all the profile names.
on-demand all	Displays information for all on-demand operations.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
ethernet-services	read

Example

This example shows how to use the **show ethernet sla operations** command:

```
RP/0/RP0:router# show ethernet sla operations
```

show ethernet sla statistics

To display the contents of buckets containing Ethernet Service Level Agreement (SLA) metrics collected by probes, use the **show ethernet sla statistics** command in EXEC mode.

show ethernet sla statistics [**current** | **history**] [**detail**] [**domain** *domain_name*] [**interface** *type R/S/I/P*] [**on-demand all**] [**profile** { *profile_name* | **all** }] [**statistic** *stat_type*]

Syntax Description

current	(Optional) Displays the content of buckets currently being filled.
history	(Optional) Displays the content of all full buckets.
domain *domain_name*	Displays information for the specified domain, where domain-name is a string of a maximum of 80 characters that identifies the domain where the SLA operation is configured.
interface *type R/S/I/P*	Displays information for the specified interface.
profile *profile_name*	Displays information for bucket for the specified profile.
profile all	Displays information for all the buckets for the specified profile names.
on-demand all	Displays information for all on-demand operations.
statistic *stat_type*	Displays only the specified type of statistic. The valid values are: • **round-trip-delay** —Displays only round-trip delay. • **round-trip-jitter** —Displays only round-trip jitter.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
ethernet-services	read

Example

This example shows how to use the **show ethernet sla statistics** command:

```
RP/0/RP0:router# show ethernet sla statistics
```

```
// Delay measurement
RP/0/RP0:ios#show ethernet sla statistics Fri Jan 17 10:09:06.855 UTC
Source: Interface FortyGigE0/5/0/9.1, Domain d1
Destination: Target MEP-ID 1
================================================================================
Profile 'p', packet type 'cfm-delay-measurement'
Scheduled to run every 1min first at 00:00:26 UTC for 1min

Round Trip Delay
~~~~~~~~~~~~~~~~
1 probes per bucket

Bucket started at 10:05:16 UTC Fri 17 January 2020 lasting 1min
    Pkts sent: 2; Lost: 0 (0.0%); Corrupt: 0 (0.0%);
                   Misordered: 1 (50.0%); Duplicates: 0 (0.0%)
    Result count: 2
    Min: 0.762ms; Max: 0.883ms; Mean: 0.822ms; StdDev: 0.060ms

    Results suspect due to a probe starting mid-way through a bucket

Bucket started at 10:05:26 UTC Fri 17 January 2020 lasting 1min
    Pkts sent: 12; Lost: 0 (0.0%); Corrupt: 0 (0.0%);
                   Misordered: 0 (0.0%); Duplicates: 0 (0.0%)
    Result count: 12
    Min: 0.599ms; Max: 0.785ms; Mean: 0.705ms; StdDev: 0.046ms

Bucket started at 10:06:26 UTC Fri 17 January 2020 lasting 1min
    Pkts sent: 12; Lost: 0 (0.0%); Corrupt: 0 (0.0%);
                   Misordered: 0 (0.0%); Duplicates: 0 (0.0%)
    Result count: 12
    Min: 0.598ms; Max: 0.850ms; Mean: 0.724ms; StdDev: 0.064ms

Bucket started at 10:07:26 UTC Fri 17 January 2020 lasting 1min
    Pkts sent: 12; Lost: 0 (0.0%); Corrupt: 0 (0.0%);
                   Misordered: 0 (0.0%); Duplicates: 0 (0.0%)
    Result count: 12
    Min: 0.599ms; Max: 0.849ms; Mean: 0.741ms; StdDev: 0.072ms


//Synthetic Loss Measurement
Source: Interface FortyGigE0/5/0/9.1, Domain d1
Destination: Target MEP-ID 1
================================================================================
Profile 'q', packet type 'cfm-synthetic-loss-measurement'
Scheduled to run every 1min first at 00:00:26 UTC for 1min Frame Loss Ratio calculated every
 1min

One-way Frame Loss (Dest->Source)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
1 probes per bucket

Bucket started at 10:08:17 UTC Fri 17 January 2020 lasting 1min
    Pkts sent: 9; Lost: 0 (0.0%); Corrupt: 0 (0.0%);
                   Misordered: 1 (11.1%); Duplicates: 0 (0.0%)
    Result count: 1
    Min: 0.000%; Max: 0.000%; Mean; 0.000%; StdDev: 0.000%; Overall: 0.000%

    Results suspect due to a probe starting mid-way through a bucket
    Results suspect as FLR calculations are based on a low packet count

Bucket started at 10:08:26 UTC Fri 17 January 2020 lasting 1min
    Pkts sent: 60; Lost: 0 (0.0%); Corrupt: 0 (0.0%);
                   Misordered: 0 (0.0%); Duplicates: 0 (0.0%)
    Result count: 1
```

```
    Min: 0.000%; Max: 0.000%; Mean; 0.000%; StdDev: 0.000%; Overall: 0.000%

Bucket started at 10:09:26 UTC Fri 17 January 2020 lasting 1min
    Pkts sent: 60; Lost: 0 (0.0%); Corrupt: 0 (0.0%);
                  Misordered: 0 (0.0%); Duplicates: 0 (0.0%)
    Result count: 1
    Min: 0.000%; Max: 0.000%; Mean; 0.000%; StdDev: 0.000%; Overall: 0.000%
```

show ethernet cfm ccm-learning-database

To display the Continuity Check Message (CCM) learning database, use the **show ethernet cfm ccm-learning-database** command in EXEC configuration mode.

show ethernet cfm ccm-learning-database [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays the CFM CCM learning database for the designated node. The *node-id* argument is entered in the *rack*/*slot*/*module* notation.

Command Default

All CFM ccm-learning-databases on all interfaces are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The CCM Learning Database is populated by MEPs and MIPs that have received continuity-check messages (CCMs). The information in the CCM Learning Database is used to reply to traceroutes when no applicable entries are found in the main MAC learning table.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display all the CFM CCM learning databases on all interfaces:

```
RP/0/RP0:hostname# show ethernet cfm ccm-learning-database

Location 0/0/RP0:

Domain/Level           Service              Source MAC     Interface
---------------------- -------------------- -------------- ------------------
foo/2                  foo                  0001.0203.0401 Te0/0/0/0
foo/2                  foo                  0001.0203.0402 PW

Location 0/1/RP0:

Domain/Level           Service              Source MAC     Interface
---------------------- -------------------- -------------- ------------------
foo/2                  foo                  0001.0203.0401 XC ID: 0xff000002
```

Table 61: show ethernet cfm ccm-learning-database Field Descriptions

Domain/Level	The domain name and the level of the domain for the maintenance point that received the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages received by maintenance points in this domain.

Service	The name of the service for the maintenance point that received the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages received by maintenance points in this domain.
Source MAC	Source MAC address in the CCM that caused this entry to be created. This entry will be used to respond to traceroute messages targeted at this MAC address.
Interface	The interface through which the CCM entered the router. This will be one of the following: • An interface or sub-interface name • A pseudowire identification (neighbor address and PW ID) • PW – Indicates the CCM was received through the PW in a cross-connect • XC ID – the internal cross-connect ID value, indicating that the CCM was received through an interface that no longer exists, or is no longer in L2 mode.

show ethernet cfm configuration-errors

To display information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred, use the **show ethernet cfm configuration-errors** command in EXEC mode.

show ethernet cfm configuration-errors [**domain** *domain-name*] [**interface** *type interface-path-id*]

Syntax Description

domain *domain-name*	(Optional) Displays information about the specified CFM domain name.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

All CFM configuration errors on all domains are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display all the CFM configuration errors on all domains:

```
RP/0/RP0:hostname# show ethernet cfm configuration-errors

Domain fig (level 5), Service bay
 * An Up MEP is configured for this domain on interface TenGigEt0/1/2/3.234 and an Up MEP
is also configured for domain blort, which is at the same level (5).
 * A MEP is configured on interface TenGigE0/3/2/1.1 for this domain/service, which has CC
 interval 100ms, but the lowest interval supported on that interface is 1s.
```

show ethernet cfm interfaces ais

To display the information about interfaces that are currently transmitting Alarm Indication Signal (AIS), use the **show ethernet cfm interfaces ais** command in EXEC mode.

show ethernet cfm interfaces [*type interface-path-id*] **ais** [**location** *node-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays information about the node location specified as *rack* / *slot* / *module*. Location cannot be specified if you configure an interface type.

Command Default

If no parameters are specified, information for all AIS interfaces is displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Note The **location** keyword cannot be specified if an interface has been specified.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to display the information published in the Interface AIS table:

```
RP/0/RP0:hostname# show ethernet cfm interfaces ais

Defects (from at least one peer MEP):
 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
```

```
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down              D - Local port down

                                Trigger                  Transmission
                          AIS   ---------    Via     ---------------------------
Interface (State)         Dir   L Defects   Levels   L Int Last started  Packets
------------------------- ---   - -------   -------  - --- ------------ ---------
Te0/1/0/0.234 (Up)        Dn    5 RPC       6        7 1s  01:32:56 ago     5576
Te0/1/0/0.567 (Up)        Up    0 M         2,3      5 1s  00:16:23 ago      983
Te0/1/0/1.1 (Dn)          Up      D                  7 60s 01:02:44 ago     3764
TE0/1/0/2 (Up)            Dn    0 RX        1!
```

Table 62: show ethernet cfm interfaces ais Field Descriptions

Interface (State)	The name and state of the interface.
AIS dir	The direction that the AIS packets are transmitted, up or down.
Trigger L	The level of the lowest MEP that is transmitting AIS.The field is blank if there are no down MEPs on the interface, and AIS is being transmitted due to configuration on the interface itself.
Trigger Defects	Defects detected by the lowest MEP transmitting AIS.
Via Levels	The levels of any MEPs on the interface that are receiving AIS from a lower MEP, and potentially re-transmitting the signal. If the highest MEP is not re-transmitting the signal, the list of levels is ended using an exclamation point.
Transmission L	The level at which AIS is being transmitted outside of the interface, via a MIP. The field is blank if this is not occurring.
Transmission Int	The interval at which AIS is being transmitted outside of the interface via a MIP. The field is blank if this is not occurring.
Transmission last started	If AIS is being transmitted outside of the interface, the time that the signal started. The field is blank if this is not occurring.
Transmission packets	If AIS is being transmitted outside of the interface, the number of packets sent by the transmitting MEP since it was created or since its counters were last cleared. The field is blank if this is not occurring.

show ethernet cfm interfaces statistics

To display the per-interface counters for Ethernet Connectivity Fault Management (CFM), use the **show ethernet cfm interfaces statistics** command in EXEC mode.

show ethernet cfm interfaces [*type interface-path-id*] **statistics** [**location** *node-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays information about the node location specified as *rack* / *slot* / *module*. Location cannot be specified if you configure an interface type.

Command Default

All CFM counters from all interfaces are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Note The location cannot be specified if a particular interface is specified.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows all the CFM counters on all interfaces:

```
RP/0/RP0:hostname# show ethernet cfm interfaces statistics
Location 0/1/RP0:

Interface              Malformed   Dropped Last Malformed Reason
-----------------      --------- --------- ---------------------
Te0/1/0/3.185                  0         0
Te0/1/0/7.185                  0         0
```

```
Te0/1/0/7.187                  0         0


RP/0/RP0:hostname# show ethernet cfm interfaces statistics
Location 0/0/RP0:

Interface              Malformed   Dropped Last Malformed Reason
-----------------      --------- --------- ---------------------
Te100/0/0/0                   10         2 Packet malformed - SLM is too short or too long
Te100/0/0/3                    4         1 Host: Packet malformed - invalid source MAC
address
                                           Satellite: Packet malformed - the format of one
 or more timestamps is invalid
```

Table 63: show ethernet cfm statistics Field Descriptions

Interface	Name of the interface.
Malformed	Number of packets that have been received at this interface that have been found to be non-compliant with the packet formats specified in IEEE 802.1ag and ITU-T Y.1731.
Dropped	Number of valid (well-formed) packets that have been received at this interface, that have been dropped in software. Packets may be dropped for the following reasons: • Packet has an unknown operation code, and reached a MEP. • Packet dropped at a MEP because it has a lower CFM level than the MEP. • Packet could not be forwarded because the interface is STP blocked. • Packet could not be forwarded because it is destined for this interface.
Last Malformed Reason	Operation code for the last malformed packet received, and the reason that it was found to be malformed. If no malformed packets have been received, this field is blank.

show ethernet cfm local maintenance-points

To display a list of local maintenance points, use the **show ethernet cfm local maintenance-points** command in EXEC mode.

show ethernet cfm local maintenance-points [{**domain** *domain-name* [**service** *service-name*] | **interface** *type interface-path-id*}] [{**mep** | **mip**}]

Syntax Description

domain *domain-name*	(Optional) Displays information about the specified domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
service *service-name*	(Optional) Displays information about the specified service, where *service-name* is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
mep	(Optional) Displays information about maintenance end points (MEPs).
mip	(Optional) Displays information about maintenance intermediate points (MIPs).

Command Default

All maintenance points from all interfaces are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read

Examples

This example shows how to display maintenance points:

```
RP/0/RP0:hostname# show ethernet cfm local maintenance-points

Domain/Level         Service             Interface         Type   ID   MAC
-------------------- ------------------- ----------------- ------ ---- --------
```

```
bar/0                bar                Te0/0/0/0          Dn MEP    1 03:04:00
baz/4                baz                Te0/0/0/1.1        MIP         03:04:01
baz/4                baz                Te0/0/0/2          MIP         03:04:02
foo/?                foo                Te0/0/0/3          MEP       1 03:04:03!
qux/2                qux                Te0/0/0/1.1        Up MEP   10 03:04:01
qux/2                qux                Te0/0/0/2          Up MEP   11 03:04:02
```

Table 64: show ethernet cfm local maintenance-points Field Descriptions

Domain/Level	The domain name and the level of the domain. If the domain is not configured globally, a question mark (?) is displayed for the Level.
Service	The name of the service.
Interface	The interface containing the maintenance point.
Type	The type of maintenance point: • MIP • Up MEP • Down MEP • MEP–If the MEP belongs to a service that is not configured globally, the type cannot be determined and just MEP is displayed.
ID	The configured MEP ID. **Note** Since MIPs do not have an ID, this column is blank for MIPs.
MAC	The last 3 octets of the interface MAC address. **Note** The first three octets are typically the Cisco OUI.
Note If the MEP has a configuration error, a exclamation point (!) is displayed at the end of the line in the display output.	

show ethernet cfm local meps

To display information about local maintenance end points (MEPs), use the **show ethernet cfm local meps** command in EXEC mode.

show ethernet cfm local meps [{**domain** *domain-name* [**service** *service-name* [**mep-id** *id*]] | **interface** *type interface-path-id* [**domain** *domain-name*]}] [{**errors** [{**detail** | **verbose**}] | **detail** | **verbose**}]

Syntax Description

domain *domain-name*	(Optional) Displays information about the specified CFM domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
service *service-name*	(Optional) Displays information about the specified service, where *service-name* is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
mep-id *id*	(Optional) Displays information about the specified MEP, where *id* is a number of a local maintenance end point (MEP). The range is 1 to 8191.
errors	(Optional) Displays information about peer MEPs with errors.
detail	(Optional) Displays detailed information.
verbose	(Optional) Displays detailed information, plus counters for each type of CFM packet.

Command Default

Brief information is displayed for all local MEPs.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

All MEPs are displayed in the **show ethernet cfm local meps** command output, unless they have configuration errors.

Task ID

Task ID	Operations
ethernet-services	read

Examples

Example 1: show ethernet cfm local meps Command

This example shows sample output of the default statistics for local MEPs without any filtering:

```
RP/0/RP0:hostname# show ethernet cfm local meps

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)             Dir MEPs/Err RD Defects AIS
----- ------------------------      --- -------- -- ------- ---
  100 Te1/1/0/1.234 (Up)            Up     0/0   N  A       L7

Domain fred (level 5), Service barney
   ID Interface (State)             Dir MEPs/Err RD Defects AIS
----- ------------------------      --- -------- -- ------- ---
    2 Te0/1/0/0.234 (Up)            Up     3/2   Y  RPC     L6

RP/0/RP0:hostname# show ethernet cfm local meps

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)             Dir MEPs/Err RD Defects AIS
----- ------------------------      --- -------- -- ------- ---
  100 Te1/1/0/1.234 (Up)            Up     0/0   N  A

Domain fred (level 5), Service barney
   ID Interface (State)             Dir MEPs/Err RD Defects AIS
----- ------------------------      --- -------- -- ------- ---
    2 Te0/1/0/0.234 (Up)            Up     3/2   Y  RPC
```

Table 65: show ethernet cfm local meps Field Descriptions

ID	Configured MEP ID of the MEP.
Interface (State)	Interface that the MEP is configured under, and the state of the interface. The states are derived from the interface state, the Ethernet Link OAM interworking state, and the Spanning Tree Protocol (STP) state. The following states are reported: • Up – Interface Up, Ethernet Link OAM Up, STP Up • Down – Interface Down or Admin Down • Blkd – Interface Up, Ethernet Link OAM Up, STP Blocked • Otherwise, the interface state.

Dir	Direction of the MEP.
RD	Remote Defect. Y (yes) indicates that a remote defect is detected on at least one peer MEP. In which case, the RDI bit is set in outgoing CCM messages. Otherwise, N (no).
MEPs	Total number of peer MEPs sending CCMs to the local MEP.
Err	Number of peer MEPs for which at least one error has been detected.
Defects	Types of errors detected. Each error is listed as a single character. Multiple errors are listed if they are from the same MEP. Possible errors are listed at the top of the display output of the command.
AIS	Alarm Indication Signal. If AIS is configured for the service, the configured level is displayed when an alarm is signaled. If AIS is not configured for the service, or if no alarm is currently signaled, this field is blank.

Example 2: show ethernet cfm local meps Command Filtered by Domain and Service

```
RP/0/RP0:hostname# show ethernet cfm local meps domain foo service bar

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)             Dir MEPs/Err RD Defects AIS
----- ------------------------      --- -------- -- ------- ---
  100 Te1/1/0/1.234 (Up)              Up     0/0   N  A       L7

RP/0/RP0:hostname# show ethernet cfm local meps domain foo service bar

 A - AIS received                I - Wrong interval
 R - Remote Defect received      V - Wrong Level
 L - Loop (our MAC received)     T - Timed out (archived)
 C - Config (our ID received)    M - Missing (cross-check)
 X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
 P - Peer port down

Domain foo (level 6), Service bar
   ID Interface (State)             Dir MEPs/Err RD Defects AIS
----- ------------------------      --- -------- -- ------- ---
  100 Te1/1/0/1.234 (Up)              Up     0/0   N  X
```

Example 3: show ethernet cfm local meps detail Command

This example shows sample output of detailed statistics for local MEPs:

Note The Discarded CCMs field is not displayed when the number is zero (0). It is unusual for the count of discarded CCMs to be anything other than zero, since CCMs are only discarded when the limit on the number of peer MEPs is reached. The Peer MEPs field is always displayed, but the counts are always zero when continuity check is not enabled.

```
RP/0/RP0:hostname# show ethernet cfm local meps detail

Domain foo (level 6), Service bar
Up MEP on TenGigE0/1/0/0.234, MEP-ID 100
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)

  CCM generation enabled:  No
  AIS generation enabled:  Yes (level: 7, interval: 1s)
  Sending AIS:             Yes (started 01:32:56 ago)
  Receiving AIS:           Yes (from lower MEP, started 01:32:56 ago)

Domain fred (level 5), Service barney
Up MEP on TenGigE0/1/0/0.234, MEP-ID 2
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 3 up, 2 with errors, 0 timed out (archived)
  Cross-check defects: 0 missing, 0 unexpected

  CCM generation enabled:  Yes (Remote Defect detected: Yes)
  CCM defects detected:    R - Remote Defect received
                           P - Peer port down
                           C - Config (our ID received)
  AIS generation enabled:  Yes (level: 6, interval: 1s)
  Sending AIS:             Yes (to higher MEP, started 01:32:56 ago)
  Receiving AIS:           No

RP/0/RP0:hostname# show ethernet cfm local meps detail

Domain foo (level 5), Service bar
Down MEP on TenGigE0/1/0/0.123, MEP-ID 20
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 1 up, 0 with errors, 0 timed out (archived)
  Cross-check errors: 0 missing, 0 unexpected

  CCM generation enabled:  Yes, 10ms
                           CCM processing offloaded to high-priority software
  AIS generation enabled:  No
  Sending AIS:             No
  Receiving AIS:           No
```

Example 4: show ethernet cfm local meps verbose Command

This example shows sample output of detailed statistics for local MEPs:

```
RP/0/RP0:hostname# show ethernet cfm local meps verbose

Domain foo (level 6), Service bar
Up MEP on TenGigE0/1/0/0.234, MEP-ID 100
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)

  CCM generation enabled:  No
  AIS generation enabled:  Yes (level: 7, interval: 1s)
  Sending AIS:             Yes (started 01:32:56 ago)
  Receiving AIS:           Yes (from lower MEP, started 01:32:56 ago)
  EFD triggered:           No
```

```
  Packet        Sent      Received
  ------  ----------  ----------------------------------------------------
  AIS           5576             0
  SLM              0            11
  SLR             11             0
  DMM              0             6
  DMR              5             0

Domain fred (level 5), Service barney
Up MEP on TenGigE0/1/0/0.234, MEP-ID 2
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 3 up, 2 with errors, 0 timed out (archived)
  Cross-check errors: 0 missing (0 auto), 0 unexpected

  CCM generation enabled:  Yes, 1s (Remote Defect detected: Yes)
                             CCM processing offloaded to software
  CCM defects detected:    R - Remote Defect received
                           P - Peer port down
                           C - Config (our ID received)
  AIS generation enabled:  Yes (level: 6, interval: 1s)
  Sending AIS:             Yes (to higher MEP, started 01:32:56 ago)
  Receiving AIS:           No

  Packet        Sent      Received
  ------  ----------  ------------------------------------------------------------
  CCM          12345         67890  (out of seq: 6, discarded: 10)
  LBM              5             0
  LBR              0             5  (out of seq: 0, with bad data: 0)
  AIS              0         46910
  LMM              3             4
  LMR              5             3

Domain gaz (level 4), Service baz
Up MEP on Standby Bundle-Ether 1, MEP-ID 3
================================================================================
  Interface state: Up      MAC address: 6655.4433.2211
  Peer MEPs: 1 up, 0 with errors, 0 timed out (archived)

  CCM generation enabled:  Yes, 1s (Remote Defect detected: No)
                             CCM processing offloaded to software
)
                           Sending disabled on local standby MEP
  CCM defects detected:    Defects below ignored on local standby MEP
                           I - Wrong interval
                           V - Wrong level

  AIS generation enabled:  No
  Sending AIS:             No
  Receiving AIS:           No

  Packet        Sent      Received
  ------  ----------  ------------------------------------------------------------
  CCM              0         67890  (out of seq: 6, discarded: 10)
  LBM              0             1
  LBR              0             2  (out of seq: 0, with bad data: 0)
  AIS              0             3
  LCK              -             4

Domain bar (level 3), Service boz
Down MEP on TenGigE102/1/0/0.345, MEP-ID 200
================================================================================
  Interface state: Up      MAC address: 1122.3344.5566
  Peer MEPs: 0 up, 0 with errors, 0 timed out (archived)
```

```
CCM generation enabled:  No
AIS generation enabled:  No
Sending AIS:             No
Receiving AIS:           No

No packets sent/received
```

show ethernet cfm peer meps

To display information about maintenance end points (MEPs) for peer MEPs, use the **show ethernet cfm peer meps** command in EXEC mode.

show ethernet cfm peer meps [{**domain** *domain-name* [**service** *service-name* [**local mep-id** *id* [**peer** {**mep-id** *id* | **mac-address** *H . H . H*}]]] | **interface** *type interface-path-id* [**domain** *domain-name* [**peer** {**mep-id** *id* | **mac-address** *H . H . H*}]]}] [{**cross-check** [{**missing** | **unexpected**}] | **errors**}] [**detail**]

Syntax Description

cross-check	(Optional) Displays information about peer MEPs with cross-check errors.
detail	(Optional) Displays detailed information.
domain *domain-name*	(Optional) Displays information about a CFM domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
errors	(Optional) Displays information about peer MEPs with errors.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
local mep-id *id*	(Optional) Displays information about a local MEP, where *id* is the number of the MEP.
missing	(Optional) Displays information about peer MEPs that are missing.
peer mep-id *id*	(Optional) Displays information about a peer MEP, where *id* is the number of the MEP.
peer mac-address *H.H.H*	(Optional) Displays information about a peer MEP, where *H.H.H* is the hexadecimal address of the MEP.
service *service-name*	(Optional) Displays information about a CFM service, where *service-name* is a string of a maximum of 154 characters that identifies the maintenance association to which the maintenance points belong.
unexpected	(Optional) Displays information about unexpected peer MEPs.

Command Default

Peer MEPs for all domains are displayed.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Note If a Local MEP is receiving Wrong Level CCMs, and if the Remote MEP has its CCM processing offloaded, then the last CCM cannot be displayed.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows sample output of MEPs detected by a local MEP:

```
RP/0/RP0:hostname# show ethernet cfm peer meps

Flags:
> - Ok                          I - Wrong interval
R - Remote Defect received      V - Wrong level
L - Loop (our MAC received)     T - Timed out
C - Config (our ID received)    M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
* - Multiple errors received

Domain dom3 (level 5), Service ser3
Down MEP on TenGigE0/0/0/0 MEP-ID 1
================================================================================
St     ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ------------ --------- ------ ----- -----
V      10 0001.0203.0403 Up      00:01:35            2      0     0     2

Domain dom4 (level 2), Service ser4
Down MEP on TenGigEt0/0/0/0 MEP-ID 1
================================================================================
St     ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ------------ --------- ------ ----- -----
 >     20 0001.0203.0402 Up      00:00:03            4      1     0     0
 >     21 0001.0203.0403 Up      00:00:04            3      0     0     0

Domain dom5 (level 2), Service dom5
```

Table 66: show ethernet cfm peer meps Field Descriptions

St	Status: one or two characters, representing the states listed at the top of the output.
ID	Peer MEP ID
MAC address	Peer MAC Address. If this entry is a configured cross-check MEP, with no MAC address specified, and no CCMs are currently being received from a peer MEP with a matching MEP ID, then this field is blank.

Port	Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.
Up/Downtime	Time since the peer MEP last came up or went down. If CCMs are currently being received, it is the time since the peer MEP last came up, which is the time since the first CCM was received. If CCMs are not currently being received, it is the time since the peer MEP last went down, which is the time since the loss threshold was exceeded and a loss of continuity was detected.
CcmRcvd	Total number of CCMs received from this peer MEP.
SeqErr	Number of CCMs received out-of-sequence.
RDI	Number of CCMs received with the RDI bit set.
Error	Number of CCMs received with CCM defects, such as: • Invalid level error • Maintenance Association Identifier (MAID) error • Interval error • Received with out MEP ID error • Invalid source MAC error

This example shows sample detailed output of MEPs detected by a local MEP:

```
RP/0/RP0:hostname# show ethernet cfm peer meps detail

Domain dom3 (level 5), Service ser3
Down MEP on TenGigE0/0/0/0 MEP-ID 1
================================================================================
Peer MEP-ID 10, MAC 0001.0203.0403
   CFM state: Wrong level, for 00:01:34
   Port state: Up
   CCM defects detected:    V - Wrong Level
   CCMs received: 5
     Out-of-sequence:             0
     Remote Defect received:      5
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              5
     Loop (our MAC received):     0
     Config (our ID received):    0
Last CCM received
     Level: 4, Version: 0, Interval: 1min
     Sequence number: 5, MEP-ID: 10
     MAID: String: dom3, String: ser3
     Port status: Up, Interface status: Up


Domain dom4 (level 2), Service ser4
Down MEP on TenGigE0/0/0/0 MEP-ID 1
================================================================================
Peer MEP-ID 20, MAC 0001.0203.0402
```

```
   CFM state: Ok, for 00:00:04
   Received CCM handling offloaded to software
   Port state: Up
   CCMs received: 7
     Out-of-sequence:             1
     Remote Defect received:      0
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              0
     Loop (our MAC received):     0
 Config (our ID received):    0
Last CCM received
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 20
     MAID: String: dom4, String: ser4
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Up

Peer MEP-ID 21, MAC 0001.0203.0403
   CFM state: Ok, for 00:00:05
   Port state: Up
   CCMs received: 6
     Out-of-sequence:             0
     Remote Defect received:      0
     Wrong Level:                 0
     Cross-connect (wrong MAID):  0
     Wrong Interval:              0
     Loop (our MAC received):     0
     Config (our ID received):    0
Last CCM received 00:00:05 ago:
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 21
     MAID: String: dom4, String: ser4
     Port status: Up, Interface status: Up


Domain dom5 (level 2), Service ser5
Up MEP on Standby Bundle-Ether 1 MEP-ID 1
================================================================================
Peer MEP-ID 600, MAC 0001.0203.0401
   CFM state: Ok (Standby), for 00:00:08, RDI received
   Port state: Down
   CCM defects detected:    Defects below ignored on local standby MEP
                            I - Wrong Interval
                            R - Remote Defect received
   CCMs received: 5
     Out-of-sequence:             0
     Remote Defect received:   5
 Wrong Level:                 0
     Cross-connect W(wrong MAID): 0
     Wrong Interval:              5
     Loop (our MAC received):     0
     Config (our ID received):    0
   Last CCM received 00:00:08 ago:
     Level: 2, Version: 0, Interval: 10s
     Sequence number: 1, MEP-ID: 600
     MAID: DNS-like: dom5, String: ser5
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Down

Peer MEP-ID 601, MAC 0001.0203.0402
   CFM state: Timed Out (Standby), for 00:15:14, RDI received
   Port state: Down
   CCM defects detected:    Defects below ignored on local standby MEP
```

```
                        I - Wrong Interval
                        R - Remote Defect received
                        T - Timed Out
                        P - Peer port down
CCMs received: 2
  Out-of-sequence:             0
  Remote Defect received:      2
  Wrong Level:                 0
  Cross-connect (wrong MAID):  0
  Wrong Interval:              2
  Loop (our MAC received):     0
  Config (our ID received):    0
Last CCM received 00:15:49 ago:
  Level: 2, Version: 0, Interval: 10s
  Sequence number: 1, MEP-ID: 600
  MAID: DNS-like: dom5, String: ser5
  Chassis ID: Local: ios; Management address: 'Not specified'
  Port status: Up, Interface status: Down
```

Table 67: show ethernet cfm peer meps detail Field Descriptions

CFM state	State of the peer MEP, how long it has been up or down, and whether the RDI bit was set in the last received CCM. The following possible states are shown if CCMs are currently being received: • Missing • Timed out—No CCMs have been received for the loss time • Ok • Indication of a defect
Port state	Port state of the peer, based on the Port Status and Interface Status TLVs. If no TLVs or CCMs have been received, this field is blank. Otherwise, the port status is displayed—unless it is Up. If the port status is Up, then the interface status is displayed.

CCM defects detected	Types of CCM defects that have been detected. The possible defects are: • Remote Defect re ceived—The last CCM received from the peer had the RDI bit set. • Loop (our MAC received)—CCMs were received from a peer with the same MAC address as the local MEP. • Config (our ID received)—CCMs were received from a peer with the same MEP ID as the local MEP. • Cross-connect (wrong MAID)—The last CCM received from the peer contained a domain/service identified that did not match the locally configured domain/service identifier. • Peer port down—The last CCM received from the peer contained an Interface Status indicating that the interface on the peer was not up. • Wrong interval—The last CCM received contained a CCM interval that did not match the locally configured CCM interval. • Wrong level—The last CCM received was for a lower level than the level of the local MEP. • Timed out—No CCMs have been received within the loss time. • Missing (cross-check)—Cross-check is configured and lists this peer MEP, but no CCMs have been received within the loss time. • Unexpected (cross-check)—Cross check is configured for this service and does not list this peer MEP, but CCMs have been received from it within the loss time.
CCMs received	Number of CCMs received in total, by defect type.
Last CCM received	How long ago the last CCM was received, and a full decode of its contents. Any unknown TLVs are displayed in hexadecimal.
Offload status	Offload status of received CCM handling.

show ethernet cfm traceroute-cache

To display the contents of the traceroute cache, use the **show ethernet cfm traceroute-cache** command in EXEC mode.

{**show ethernet cfm traceroute-cache** [[**domain** *domain-name*] [**service** *service-name*] [**local mep-id** *id*] [**transaction-id** *id*]] | **interface** *type interface-path-id* [[**domain** *domain-name*] [**transaction-id** *id*]] [{**exploratory** | **targeted**}] [**status** {**complete** | **incomplete**}] [**detail**]}

Syntax Description

domain *domain-name*	(Optional) Displays information about a CFM domain, where *domain-name* is a string of a maximum of 80 characters that identifies the domain in which the maintenance points reside.
service *service-name*	(Optional) Displays information about a CFM service, where *service-name* is a string of a maximum of 80 characters that identifies the maintenance association to which the maintenance points belong.
local mep-id *id*	(Optional) Displays information for the specified local maintenance end point (MEP). The range for MEP ID numbers is 1 to 8191.
transaction-id *id*	(Optional) Displays information for the specified transaction.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
exploratory	(Optional) Displays information for exploratory traceroutes.
targeted	(Optional) Displays information for traceroutes that are not exploratory, but explicitly mapped.
status	(Optional) Displays status information.
complete	(Optional) Displays status information for traceroutes that have received all replies.
incomplete	(Optional) Displays status information for traceroutes that are still receiving replies.
detail	(Optional) Displays detailed information.

Command Default

Shows output for the default traceroute.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show ethernet cfm traceroute-cache** command to display the contents of the traceroute cache; for example, to see the maintenance intermediate points (MIPs) and maintenance end points (MEPs) of a domain as they were discovered. The data is historic. The traceroute cache stores entries from previous traceroute operations.

In the output, the traceroutes sourced from each local MEP are listed. The heading for the local MEP contains the domain name and level, service name, MEP ID and interface name.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows sample output for the **show ethernet cfm traceroute-cache** command:

```
RP/0/RP0:hostname# show ethernet cfm traceroute-cache

Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface TenGigE0/0/0/0
================================================================================
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402,
TTL 64, Trans ID 2:

Hop Hostname/Last            Ingress MAC/name       Egress MAC/Name        Relay
--- ------------------------ ---------------------- ---------------------- -----
  1 ios                      0001.0203.0400 [Down]                         FDB
      0000-0001.0203.0400    Te0/0/0/0
  2 abc                                             0001.0203.0401 [Ok]    FDB
      ios                                           Not present
  3 bcd                      0001.0203.0402 [Ok]                           Hit
      abc                    Te0/0
Replies dropped: 0


Traceroutes in domain foo (level 2), service foo
Source: MEP-ID 1, interface TenGigE0/0/0/0
================================================================================
Traceroute at 2009-05-18 12:03:31 to 0001.0203.0403,
TTL 64, Trans ID 1:

Hop Hostname/Last            Ingress MAC/name       Egress MAC/Name        Relay
--- ------------------------ ---------------------- ---------------------- -----
  1 abc                      0001.0203.0401 [Ok]                           FDB
      0000-0001.0203.0400    Not present
  2 bob                      0001.0203.0402 [Ok]                           MPDB
      abc                    Te0/1/0/2.3
  3 cba                                             0001.0203.0403 [Ok]    Hit
      bob                                           Te0/2/0/3.45
Replies dropped: 0


Traceroute at 2009-05-18 12:15:47 to 0001.0203.0409,
TTL 64, Trans ID 3, automatic:
00:00:05 remaining
```

```
Traceroute at 2009-05-18 12:20:10 explore to ffff.ffff.ffff,
TTL 64, Trans ID 4, Timeout auto, Reply Filter Default:

Hop               Hostname/Last            Ingr/Egr MAC/name               Relay
----------------- ------------------------ -------- ---------------------- -----
1                 abc                      Ingress  0015.0000.323f [Ok]    FDB
                    0000-0001.0203.0400             Te0/0/0/0.1
 2                abc                      Egress   0015.0000.323e [Ok]    FDB
                    abc                             Te0/1/0/0.1
  3               0002-0016.eeee.1234      Ingress  0016.eeee.1234 [Ok]    FDB
                    abc                             Te0/4.23
   4              0000-0016.eeee.4321      Egress   0016.eeee.4321 [Ok]    FDB
                    0002-0016.eeee.1234             Te1/2.23
    5             rtr                      Ingress  0015.0000.f123 [Ok]    FDB
                    0002-00.16.eeee.4321            Te0/0/0/0
 2                abc                      Egress   0015.0000.323d [Ok]    FDB
                    abc                             Te0/1/0/1.1
  3               pe2                      Ingress  0017.0000.cf01 [Ok]    FDB
                    abc                             Te0/0/2/0/1.450
   4              pe2                      Egress   0017.0000.cf01 [Ok]    Drop
                    pe2                             Te0/0/0/0.451
   4              pe2                      Egress   0017.0000.cf01 [Ok]    FDB
                    pe2                             Te0/0/0/1.452
    5             ce2                      Ingress  0015.0000.8830 [Ok]    FDB
                    pe2                             Te0/1/0/0
Replies dropped: 0
```

Table 68: show ethernet cfm traceroute-cache Field Descriptions

Field	Description
Traceroute at	Date and time the traceroute was started.
to	Destination MAC address.
explore to	(Exploratory traceroutes) MAC address of the target for the exploratory traceroute.
TTL	Initial Time To Live used for the traceroute operation.
Trans ID	Transaction ID
Timeout	(Exploratory traceroutes) If no timeout was configured, “Timeout auto” is shown.
Reply Filter	(Exploratory traceroutes) Type of filter.
automatic	Indicates that the traceroute was triggered automatically (for example, as a result of a peer MEP exceeding the loss threshold, or if Continuity-Check Auto-traceroute is configured).
00:00:00 remaining	If the traceroute is in progress, the time remaining until it completes.
No replies received	Traceroute has completed but no replies were received.
Replies dropped	Number of replies dropped.
FDB only	Indicates FDB-only was configured for a standard traceroute.

Field	Description
Hop	Number of hops between the source MEP and the Maintenance Point that sent the reply. (Exploratory traceroutes) The display is indented by an extra character as the hop increases, so that the tree of responses can be seen.
Hostname/Last	On the first line, the hostname of the Maintenance Point that sent the reply. On the second line, the hostname of the previous Maintenance Point in the path. If either of the hostnames is unknown, the corresponding Egress ID is displayed instead.
Ingr/Egr	(Exploratory traceroutes) Indicates whether the reply is for an ingress or egress interface, but never both.
Ingress MAC/Name	If the reply includes information about the ingress interface, then the first line displays the ingress interface MAC address and the ingress action. The ingress interface name, if known, is displayed on the second line.
Egress MAC/Name	If the reply includes information about the egress interface, then the first line displays the egress interface MAC address and the egress action. The egress interface name, if known, is displayed on the second line.
MAC/Name	(Exploratory traceroutes) The MAC address of the interface from which the reply was sent, and the ingress/egress action, are displayed on the first line. If the interface name was present in the reply, it is displayed on the second line.
Relay	Type of relay action performed. For standard traceroutes, the possible values are: • Hit—The target MAC address was reached. • FDB—The target MAC address was found in the Filtering Database (the MAC learning table on the switch) and will be forwarded by the interface. • MPDB—The target MAC address was found in the MP Database (the CCM Learning database on the switch). In addition, “MEP” is displayed on the second line if a terminal MEP was reached. For exploratory traceroutes, the possible values are: • Hit—The target MAC address was reached. • FDB—The target MAC address was found in the Filtering Database and will be forwarded at this interface. • Flood—The target MAC address was not found in the Filtering database, and will be flooded at this interface. • Drop—The target MAC address will not be forwarded at this interface.

The following example shows sample output for the **show ethernet cfm traceroute-cache detail** command:

```
RP/0/RP0:hostname# show ethernet cfm traceroute-cache domain bar detail

Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface TenGigE0/0/0/0
================================================================================
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402,
TTL 64, Trans ID 2:

Hop Hostname                 Ingress MAC            Egress MAC             Relay
--- ------------------------ ---------------------- ---------------------- -----
  1 ios                      0001.0203.0400 [Down]                         FDB
        Level: 4, version: 0, Transaction ID: 2
        TTL: 63, Relay Action: RlyFDB
        Forwarded, Terminal MEP not reached
        Last egress ID: 0000-0001.0203.0400
        Next egress ID: 0000-0001.0203.0400
        Ingress interface:
          Action: IngDown, MAC: 0001.0203.0400
          ID: Local: Te0/0/0/0
        Hostname: Local: ios, address Not specified

  2 abc                                                0001.0203.0401 [Ok]   FDB
        Level: 4, version: 0, Transaction ID: 2
        TTL: 62, Relay Action: RlyFDB
        Forwarded, Terminal MEP not reached
        Last egress ID: 0000-0001.0203.0400
        Next egress ID: 0000-0001.0203.0401
        Egress interface:
          Action: EgOk, MAC: 0001.0203.0401
          ID: Not present
        Hostname: Local: abc, address Not specified

  3 bcd                      0001.0203.0402 [Ok]                           Hit
        Level: 4, version: 0, Transaction ID: 2
        TTL: 61, Relay Action: RlyHit
        Not Forwarded, Terminal MEP not reached
        Last egress ID: 0000-0001.0203.0401
        Next egress ID: Not Forwarded
        Ingress interface:
          Action: IngOk, MAC: 0001.0203.0402
          ID: Local: TenGigE0/0
        Hostname: Local: bcd, address Not specified

Replies dropped: 0


Traceroute at 2009-05-18 12:30:10 explore to ffff.ffff.ffff from 0204.0608.0a0c,
TTL 255, Trans ID 5, Timeout auto, Reply Filter Spanning Tree:

Hop Hostname                           Ingr/Egr MAC                    Relay
--- ---------------------------------- -------- ---------------------- -----
  1 0000-0015.0000.fffe                Ingress  0015.0000.fffe [Ok]    FDB
        Level: 2, version: 0, Transaction ID: 5
        TTL: 254, Relay Action: RlyFDB
        Forwarded, Terminal MEP not reached
        Next-Hop Timeout: 5 seconds
        Delay Model: Logarithmic
        Last egress ID: 0000-0002.0002.0002
        Next egress ID: 0000-0015.0000.fffe
        Ingress interface:
          Action: ELRIngOk, MAC: 0015.0000.fffe
          ID: Local: Te0/0/0/0.1
```

```
2 0001-0030.0000.fffd                    Egress   0030.0000.fffd [Ok]    Drop
       Level: 2, version: 0, Transaction ID: 5
       TTL: 253, Relay Action: RlyDrop
       Not Forwarded, Terminal MEP not reached
       Next-Hop Timeout: 5 seconds
       Delay Model: Logarithmic
       Last egress ID: 0000-0015.0000.fffe
       Next egress ID: 0030-0000.0000.fffd
       Egress interface:
         Action: ELREgrOk, MAC: 0030.0000.fffd
         ID: Local: Te0/1/0/1.2
```

show ethernet lmi interfaces

To display Ethernet Local Management Interface (E-LMI) information for an interface, including protocol status and error and event statistics, use the **show ethernet lmi interfaces** command in EXEC configuration mode.

show ethernet lmi interfaces [*type interface-path-id*][**brief** | **detail**]
show ethernet lmi interfaces [**brief** | **detail**][**location** *location*]

Syntax Description

brief	(Optional) Displays summary information about the E-LMI protocol status, number of EVCs and errors, and CE-VLAN/EVC map type.
detail	(Optional) Displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred, including details about subinterfaces and EVC status.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *location*	(Optional) Displays E-LMI information for the designated node. The *location* argument is entered in the *rack*/*slot*/*module* notation. **Note** The location cannot be specified when you specify an interface type.

Command Default

The output displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred since the protocol was enabled on the interface or counters were cleared.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If Protocol Errors are seen in the output, then the CE device is sending packets to the PE device, but the PE does not understand those packets. This suggests an incorrect implementation of the E-LMI protocol on the CE side, or corruption of the packets on the path between the CE and PE. E-LMI packets have a strictly defined

structure in the MEF 16 standard, and any deviation from that results in a protocol error. The PE will not respond to any packets that are malformed and result in a protocol error.

The Reliability Error counters can indicate that messages are being lost between the PE and CE devices. The timers in the last block of the output should indicate that messages are being sent and received by the PE device. Consider the following actions when these Reliability Errors occur:

- Status Enq Timeouts—If this counter is continuously incrementing, it indicates that the Polling Timer on the CE is configured to a greater value than the PVT configuration on the PE. Status Enquiry messages will be sent less frequently than the PVT expects them and PVT timeouts occur. Be sure that the value of the PVT (specified by the **polling-verification-timer** command on the PE) is greater than the Polling Timer value on the CE device.
- Invalid Sequence Number—Indicates that messages from the PE are not being received by the CE. Be sure that the correct interface on the CE device is connected to the corresponding E-LMI interface on the PE device, so that communication can take place. Verify that both interfaces are Up.
- Invalid Report Type—This error can occur under the following conditions:
  - If the protocol is in the process of a status update and an "E-LMI Check" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.
  - If the protocol is not in the process of a status update and a "Full Status Continued" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.

Note If the protocol is in the process of a status update and a "Full Status" type of STATUS ENQUIRY is received by the PE, then the PE restarts the status update but does not record any error.

Task ID

Task ID	Operation
ethernet-services	read

The following example shows sample output for the default form of the command:

```
RP/0/RP0:hostname# show ethernet lmi interfaces
Interface: TenGigE0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128

  Reliability Errors:
    Status Enq Timeouts                19 Invalid Sequence Number            0
    Invalid Report Type                 0

  Protocol Errors:
    Malformed PDUs                      0 Invalid Protocol Version           0
    Invalid Message Type                0 Out of Sequence IE                 0
    Duplicated IE                       0 Mandatory IE Missing               0
    Invalid Mandatory IE                0 Invalid non-Mandatory IE           0
    Unrecognized IE                     0 Unexpected IE                      0
```

```
Full Status Enq Rcvd     00:00:10 ago   Full Status Sent      00:00:10 ago
PDU Rcvd                 00:00:00 ago   PDU Sent              00:00:00 ago
LMI Link Status Changed  10:00:00 ago   Last Protocol Error      never
Counters cleared            never
```

Table 69: show ethernet lmi interfaces Field Descriptions

Field	Description
Interface:	Name of the interface running the E-LMI protocol.
Ether LMI Link Status:	Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).
UNI Id:	Name of the UNI as configured by the **ethernet uni id** command. This output field does not appear if the UNI ID is not configured.
Line Protocol State:	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
MTU (*x* PDUs reqd for full report)	Maximum Transmission Unit of the interface and the number (*x*) of E-LMI PDUs of that size required to send one full status report.
CE-VLAN/EVC Map Type: *type* (*x* EVCs)	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible valued for *type* are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number *x* of EVCs in the map are displayed in parentheses.
Configuration: Status counter	Value of the MEF N393 Status Counter as configured by the **status-counter** command.
Polling Verification Timer	Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the **polling-verification-timer** command. Displays "disabled" if the PVT is turned off.
Last Data Instance Sent:	Current value of the Data Instance.
Last Sequence Numbers: Sent *x*, Received *y*	Values of the last sent (*x*) and received (*y*) sequence numbers as reported in sent PDUs.

Field	Description
Reliability Errors:	Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared: • Status Enq Timeouts—Increments every time the Polling Verification Timer (PVT) expires. • Invalid Report Type—Increments if the Report Type is not appropriate to the protocol's current state. There are four Report Types defined by the E-LMI Standard, and only three of them can appear in Status Enquiry messages that the PE receives. These are: E-LMI Check, Full Status and Full Status Continued. • Invalid Sequence Number—Increments whenever the received sequence number in a Status Enquiry from the CE does not match the last sent sequence number in the PE response. Indicates that messages from the PE are not being received by the CE. The PE continues to respond with the requested Report Type. For more information about possible actions, see the "Usage Guidelines" section.
Protocol Errors: (Malformed PDUs, Invalid Message Type, Duplicated IE, and others)	Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.
Full Status Enq Rcvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.	Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays "never" if the event has not occurred since the protocol was enabled on the interface or counters were cleared.

The following example shows sample output for the **show ethernet lmi interfaces brief** form of the command:

```
RP/0/RP0:hostname# show ethernet lmi interfaces brief
                     ELMI   LineP      #            CE-VLAN/
Interface            State  State      EVCs  Errors EVC Map
-------------------------------------------------------------------------------
Te0/0/0/0            Up     Up            3      19 Multiplexing, no bundling
Te0/0/0/1            Down   Admin-down    1       0 All to One Bundling
```

Table 70: show ethernet lmi interfaces brief Field Descriptions

Field	Description
Interface	Name of the interface running the E-LMI protocol.

Field	Description
ELMI State	Status of the E-LMI protocol. Possible values are Up, Down, or N/A if the Polling Verification Timer is disabled.
LineP State	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
# EVCs	Total number of EVCs in the CE-VLAN/EVC map.
Errors	Total number of reliability and protocol errors encountered since the protocol was enabled on the interface or counters were cleared.
CE-VLAN/EVC Map	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible values are Bundling, All to One Bundling, or Multiplexing, no bundling.

The following example shows sample output for the **show ethernet lmi interfaces detail** form of the command:

```
RP/0/RP0:hostname #show ethernet lmi interfaces detail
Interface: TenGigE0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128

  Reliability Errors:
    Status Enq Timeouts                 19 Invalid Sequence Number             0
    Invalid Report Type                  0

  Protocol Errors:
    Malformed PDUs                       0 Invalid Protocol Version            0
    Invalid Message Type                 0 Out of Sequence IE                  0
    Duplicated IE                        0 Mandatory IE Missing                0
    Invalid Mandatory IE                 0 Invalid non-Mandatory IE            0
    Unrecognized IE                      0 Unexpected IE                       0

  Full Status Enq Rcvd     00:00:10 ago   Full Status Sent      00:00:10 ago
  PDU Rcvd                 00:00:00 ago   PDU Sent              00:00:00 ago
  LMI Link Status Changed  10:00:00 ago   Last Protocol Error      never
  Counters cleared            never

  Sub-interface: TenGigE0/0/0/0.1
    VLANs: 1,10,20-30, default, untagged/priority tagged
    EVC Status: New, Partially Active
    EVC Type: Multipoint-to-Multipoint
    OAM Protocol: CFM
      CFM Domain: Global (level 5)
      CFM Service: CustomerA
    Remote UNI Count: Configured = 2, Active = 1

    Remote UNI Id                                                    Status
```

```
-------------                                                   ------
PE2-CustA-Slot2-Port2                                           Up
PE2-CustA-Slot3-Port3                                           Unreachable
```

Table 71: show ethernet lmi interfaces detail Field Descriptions

Field	Description
Interface:	Name of the interface running the E-LMI protocol.
Ether LMI Link Status:	Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).
UNI Id:	Name of the UNI as configured by the **ethernet uni id** command. This output field does not appear if the UNI ID is not configured.
Line Protocol State:	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
MTU (*x* PDUs reqd for full report)	Maximum Transmission Unit of the interface and the number (*x*) of E-LMI PDUs of that size required to send one full status report.
CE-VLAN/EVC Map Type: *type* (*x* EVCs)	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible valued for *type* are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number *x* of EVCs in the map are displayed in parentheses.
Configuration: Status counter	Value of the MEF N393 Status Counter as configured by the **status-counter** command.
Polling Verification Timer	Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the **polling-verification-timer** command. Displays "disabled" if the PVT is turned off.
Last Data Instance Sent:	Current value of the Data Instance.
Last Sequence Numbers: Sent *x*, Received *y*	Values of the last sent (*x*) and received (*y*) sequence numbers as reported in sent PDUs.
Reliability Errors: (Status Enq Timeouts, Invalid Report Type, and Invalid Sequence Number)	Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared.
Protocol Errors: (Malformed PDUs, Invalid Message Type, Duplicated IE, and others)	Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.

Field	Description
Full Status Enq Rcvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.	Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays "never" if the event has not occurred since the protocol was enabled on the interface or counters were cleared.
Subinterface:	Name of the subinterface corresponding to the EVC.
VLANs:	VLAN traffic on the interface that corresponds to the EFPs encapsulation, with the following possible values: • Numbers of the matching VLAN IDs **Note** If Q-in-Q encapsulation is configured, only the outer tag is displayed. • default—Indicates that Default tagging is configured, or the encapsulation specifies to match "any." • none—No matches for the configured encapsulation have occurred on the interface. • untagged/priority—Traffic is either untagged or has priority tagging. **Note** If the message "EVC omitted from Full Status due to encapsulation conflict" is displayed above the VLAN output, a misconfiguration has occurred with two or more EFPs having a conflicting encapsulation.
EVC Status:	State of the EVC, with the following possible values: • Active—E-LMI is operational for this EVC. • Inactive—All of the remote UNIs are unreachable or down. • New—The EVC has not yet been reported to the CE device. • Not yet known—E-LMI is still waiting to receive the status from CFM. This condition should not persist for more than a few seconds. • Partially Active—One or more of the remote UNIs is unreachable or down.
EVC Type:	Type of the EVC, with the following possible values: "Point-to-Point," "Multipoint-to-Multipoint," or "EVC type not yet known."

Field	Description
OAM Protocol:	The OAM protocol from which the EVC status and type are derived. Possible values are either "CFM" or "None."
CFM Domain:	Name of the CFM domain for this EVC.
CFM Service:	Name of the CFM service for this EVC.
Remote UNI Count: Configured = *x*, Active = *y*	Number of configured or expected remote UNIs (*x*) and the number of active remote UNIs (*y*) within the EVC.
Remote UNI Id:	ID of each remote UNI, including both configured and active remote UNIs where these two sets are not identical. If the number of configured and active remote UNIs is zero, no table is displayed. **Note** Where no ID is configured for a remote UNI using the **ethernet uni id** command, then the CFM remote MEP ID is displayed, for example, "<Remote UNI Reference Id: *x*>"
Status	Status of each remote UNI, with the following possible values: "Up," "Down," "Admin Down," "Unreachable (a configured remote UNI is not active or missing)," or "Unknown (a remote UNI is active but not reporting its status)."

show ethernet oam configuration

To display the current active Ethernet OAM configuration on an interface, use the **show ethernet oam configuration** command.

show ethernet oam configuration [**interface** *type interface-path-id*]

Syntax Description

interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

If no parameters are specified, the configurations for all Ethernet OAM interfaces is displayed.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command displays the Ethernet OAM configuration information for all interfaces, or a specified interface.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display Ethernet OAM configuration information for a specific interface:

```
RP/0/RP0:hostname# show ethernet oam configuration interface TenGigE0/4/0/0
Thu Aug  5 21:54:34.050 DST
TenGigE0/4/0/0:
  Hello interval:                                          1s
  Link monitoring enabled:                                  N
  Remote loopback enabled:                                  N
  Mib retrieval enabled:                                    N
  Uni-directional link-fault detection enabled:             N
  Configured mode:                                     Active
  Connection timeout:                                       5
  Symbol period window:                                     0
  Symbol period low threshold:                              1
  Symbol period high threshold:                          None
  Frame window:                                          1000
  Frame low threshold:                                      1
  Frame high threshold:                                  None
  Frame period window:                                   1000
```

```
  Frame period low threshold:                                1
  Frame period high threshold:                            None
  Frame seconds window:                                  60000
  Frame seconds low threshold:                               1
  Frame seconds high threshold:                           None
  High threshold action:                                  None
  Link fault action:                                       Log
  Dying gasp action:                                       Log
  Critical event action:                                   Log
  Discovery timeout action:                                Log
  Capabilities conflict action:                            Log
  Wiring conflict action:                          Error-Disable
  Session up action:                                       Log
  Session down action:                                     Log
  Remote loopback action:                                  Log
  Require remote mode:                                  Ignore
  Require remote MIB retrieval:                              N
  Require remote loopback support:                           N
  Require remote link monitoring:                            N
```

The following example shows how to display the configuration for all EOAM interfaces:

```
RP/0/RP0:hostname# show ethernet oam configuration
Thu Aug  5 22:07:06.870 DST
TenGigE0/4/0/0:
  Hello interval:                                           1s
  Link monitoring enabled:                                   N
  Remote loopback enabled:                                   N
  Mib retrieval enabled:                                     N
  Uni-directional link-fault detection enabled:              N
  Configured mode:                                      Active
  Connection timeout:                                        5
  Symbol period window:                                      0
  Symbol period low threshold:                               1
  Symbol period high threshold:                           None
  Frame window:                                           1000
  Frame low threshold:                                       1
  Frame high threshold:                                   None
  Frame period window:                                    1000
  Frame period low threshold:                                1
  Frame period high threshold:                            None
  Frame seconds window:                                  60000
  Frame seconds low threshold:                               1
  Frame seconds high threshold:                           None
  High threshold action:                                  None
  Link fault action:                                       Log
  Dying gasp action:                                       Log
  Critical event action:                                   Log
  Discovery timeout action:                                Log
  Capabilities conflict action:                            Log
  Wiring conflict action:                          Error-Disable
  Session up action:                                       Log
  Session down action:                                     Log
  Remote loopback action:                                  Log
  Require remote mode:                                  Ignore
  Require remote MIB retrieval:                              N
  Require remote loopback support:                           N
  Require remote link monitoring:                            N
```

show ethernet oam discovery

To display the currently configured OAM information of Ethernet OAM sessions on interfaces, use the **show ethernet oam discovery**.

show ethernet oam discovery [{**brief** | **interface** *type* *interface-path-id* [**remote**]}]

Syntax Description

brief	Displays minimal, currently configured OAM information in table form.
interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
remote	(Optional) Retrieves and displays information from a remote device, as if the command was run on the remote device.

Command Default

Displays detailed information for Ethernet OAM sessions on all interfaces.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display the minimal, currently configured OAM information for Ethernet OAM sessions on all interfaces:

```
RP/0/RP0:hostname# show ethernet oam discovery brief

Sat Jul  4 13:52:42.949 PST
Flags:
    M - MIB Retrieval support
    U - Unidirectional detection support
    * - data is unavailable

Local                  Remote         Remote
Interface              MAC Address    Vendor Mode    Capability
---------------------- -------------- ------ ------- ----------
Te0/1/5/1              0010.94fd.2bfa 00000A Active  L
Te0/1/5/2              0020.95fd.3bfa 00000B Active  M
Te0/1/6/1              0030.96fd.6bfa 00000C Passive L R
```

The following example shows how to display detailed, currently configured OAM information for the Ethernet OAM session on a specific interface:

```
RP/0/RP0:hostname# show ethernet oam discovery interface TenGigE0/1/5/1

Sat Jul  4 13:56:49.967 PST
TenGigE0/1/5/1:
Local client
------------
  Administrative configuration:
    PDU revision:                       1
    Mode:                          Active
    Unidirectional support:             N
    Link monitor support:               N
    Remote loopback support:            N
    MIB retrieval support:              N
    Maximum PDU size:                1500
    Mis-wiring detection key:        5E9D

Operational status:
    Port status:               Active send
    Loopback status:                 None
    Interface mis-wired:                N

Remote client
-------------
  MAC address:              0030.96fd.6bfa
  Vendor (OUI):          00.00.0C (Cisco)

  Administrative configuration:
    PDU revision:                       5
    Mode:                          Passive
    Unidirectional support:             N
    Link monitor support:               N
    Remote loopback support:            N
    MIB retrieval support:              N
    Maximum PDU size:                1500
```

show ethernet oam interfaces

To display the current state of Ethernet OAM interfaces, use the **show ethernet oam interfaces** command.

show ethernet oam interfaces [**interface** *type* *interface-path-id*]

Syntax Description

interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No parameters displays the current state for all Ethernet OAM interfaces.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display the current state for all Ethernet OAM interfaces:

```
RP/0/RP0:hostname# show ethernet oam interfaces
TenGigE0/0/0/0
In REMOTE_OK state
Local MWD key: 80081234
Remote MWD key: 8F08ABCC
EFD triggered: Yes (link-fault)
```

Table 72: show ethernet oam interfaces Field Descriptions

Field	Description
In *type* state	The possible discovery state *type* values are: • ACTIVE_SEND_LOCAL—The interface is configured in active mode (the default), but no Information PDUs have been received from the peer (except possibly link-fault PDUs). Information PDUs are sent. • FAULT—A local unidirectional link fault has been detected. Link-fault PDUs are sent. • INACTIVE—The interface is down. • PASSIVE_WAIT—The interface is configured in passive mode (**mode passive** command) but no Information PDUs have been received from the peer (except possibly link-fault PDUs). No PDUs are sent. • REMOTE—(Also known as SEND_LOCAL_REMOTE). Information PDUs are being sent and received, but the local device is not satisfied with the remote peer's capabilities (for example, because there is a 'require-remote' configuration and the peer does not have the required capabilities). • REMOTE_OK—(Also known as SEND_LOCAL_REMOTE_OK). Information PDUs are being sent and received, and the local device is satisfied with the peer's capabilities, but the remote peer is not satisfied with the local device capabilities (for example, because there is a 'require-remote' configuration on the peer device). • SEND_ANY—The discovery process has completed, both devices are satisfied with the configuration and the session is up. All types of PDU can be sent and received.
EFD triggered	Indicates if an Ethernet Fault Detection (EFD) event has occurred on the interface and the type of fault that triggered the interface to be moved to the down state for the line protocol. The possible EFD trigger events are: • capabilities-conflict • discovery-timeout • link-fault • session-down • wiring-conflict

show ethernet oam statistics

To display the local and remote Ethernet OAM statistics for interfaces, use the **show ethernet oam statistics** command.

show ethernet oam statistics [**interface** *type interface-path-id* [**remote**]]

Syntax Description

interface *type*	(Optional) Displays information about the specified interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
remote	(Optional) Retrieves and displays information from a remote device, as if the command was run on the remote device.

Command Default

No parameters displays statistics for all Ethernet OAM interfaces.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read

Examples

The following example shows how to display Ethernet OAM statistics for a specific interface:

```
RP/0/RP0:hostname# show ethernet oam statistics interface TenGigE0/1/5/1

TenGigE0/1/5/1:
Counters
--------
    Information OAMPDU Tx                        161177
    Information OAMPDU Rx                        151178
    Unique Event Notification OAMPDU Tx               0
    Unique Event Notification OAMPDU Rx               0
    Duplicate Event Notification OAMPDU Tx            0
    Duplicate Event Notification OAMPDU Rx            0
    Loopback Control OAMPDU Tx                        0
    Loopback Control OAMPDU Rx                        0
    Variable Request OAMPDU Tx                        0
    Variable Request OAMPDU Rx                        0
    Variable Response OAMPDU Tx                       0
    Variable Response OAMPDU Rx                       0
    Organization Specific OAMPDU Tx                   0
    Organization Specific OAMPDU Rx                   0
    Unsupported OAMPDU Tx                            45
    Unsupported OAMPDU Rx                             0
    Frames Lost due to OAM                           23
```

```
    Fixed frames Rx                                 1

Local event logs
----------------
    Errored Symbol Period records                   0
    Errored Frame records                           0
    Errored Frame Period records                    0
    Errored Frame Second records                    0

Remote event logs
-----------------
    Errored Symbol Period records                   0
    Errored Frame records                           0
    Errored Frame Period records                    0
    Errored Frame Second records                    0
```

snmp-server traps ethernet cfm

To enable SNMP traps for Ethernet Connectivity Fault Management (CFM), use the **snmp-server traps ethernet cfm** command in global configuration mode.

snmp-server traps ethernet cfm

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet OAM event traps are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If a Local MEP is receiving Wrong Level CCMs, then a transient timeout might occur when correct Level CCMs are received again.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable SNMP server traps on an Ethernet OAM interface.

```
RP/0/RP0:hostname #configure
RP/0/RP0:hostname(config)# snmp-server traps ethernet cfm
```

snmp-server traps ethernet oam events

To enable SNMP traps for Ethernet OAM events, use the **snmp-server traps ethernet oam events** command.

snmp-server traps ethernet oam events

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet OAM event traps are not enabled.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable SNMP server traps on an Ethernet OAM interface.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# snmp-server traps ethernet oam events
```

status-counter

To set the Metro Ethernet Forum (MEF) N393 Status Counter value that is used to determine Ethernet Local Management Interface (E-LMI) operational status, use the **status-counter** command in interface Ethernet LMI configuration mode. To return to the default, use the **no** form of the command.

status-counter *threshold*
no status-counter *threshold*

Syntax Description

threshold	Number from 2 to 10. The default is 4.

Command Default

The N393 Status Counter is set to 4.

Command Modes

Interface Ethernet LMI configuration (config-if-elmi)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If the E-LMI protocol status is currently Up, the Status Counter specifies how many consecutive times the PVT must expire before the status is changed to Down. If the E-LMI status is currently Down, the Status Counter specifies how many STATUS ENQUIRY messages must be received without the PVT expiring before the status is changed to Up. If the PVT is disabled, the status counter has no effect.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to set the MEF Status Counter for E-LMI to 6:

```
RP/0/RP0:hostname# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if-elmi)# status-counter 6
```

tags

To set the number of outer tags in CFM packets sent from up MEPs in a CFM domain service, use the **tags** command in CFM domain service configuration mode. To return the number of tags in CFM packets to the default value, use the **no** form of this command.

tags *number*
no tags *number*

Syntax Description

number	Specifies the number of tags in CFM packets from up MEPs. Currently, the only valid value is 1.

Command Default

When not configured, CFM packets are sent with the same number of tags as customer data traffic, according to the encapsulation and rewrite configuration.

Command Modes

CFM domain service configuration (config-cfm-dmn-svc)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command allows you to set the number of tags in CFM packets from up MEPs to 1, so that the system can differentiate between CFM packets and data packets. When not configured, CFM packets from UP MEPs have the same number of tags as data packets, and consequently, may not be forwarded to the appropriate route.

Tags can be configured only for services that are associated with a cross-connect.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to set the number of tags in CFM packets from up MEPs in a CFM domain service:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain D1 level 1
RP/0/RP0:hostname(config-cfm-dmn)# service S2 xconnect group grp1 p2p xc1
RP/0/RP0:hostname(config-cfm-dmn-svc)# tags 1
```

traceroute cache

To set the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries, use the **traceroute cache** command in CFM configuration mode. To return the traceroute cache to its default limits, use the **no** form of this command.

traceroute cache hold-time *minutes* **size** *entries*
no traceroute cache hold-time *minutes* **size** *entries*

Syntax Description

hold-time *minutes*	Timeout value in minutes that entries are held in the Ethernet CFM traceroute cache table before being cleared. Range is 1 minute or greater.
size *entries*	Maximum number of entries that are stored in the Ethernet CFM traceroute cache table. An entry is a single traceroute reply. Range is 1 to 5000.

Command Default

hold-time: 100

size: 100

Command Modes

CFM configuration (config-cfm)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

A separate cache is managed for each node that sends a traceroute request. All replies to a single traceroute request are cached at once. The **hold-time** begins when the last reply to a request is received. When the **hold-time** limit is reached, all replies to that request are cleared. The size of each traceroute reply is limited by the MTU of the interface.

When the maximum number of entries (**size** *entries*) is exceeded, all replies for the oldest request are deleted.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to set the **hold-time** and the **size** of a traceroute cache.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# traceroute cache hold-time 1 size 3000
```

traceroute ethernet cfm

To send Ethernet connectivity fault management (CFM) traceroute messages to generate a basic, targeted, or exploratory traceroute, use the **traceroute ethernet** command in EXEC mode.

traceroute ethernet cfm domain *domain-name* **service** *service-name* {**mac-address** *target-mac-address* | **mep-id** *target-mep-id* | **explore** [**all-ports**] [**from** *from-mac-address*]} **source** [**mep-id** *source-mep-id*] **interface** *type interface-path-id* [**asynchronous**] [**timeout** *seconds*] [**filtering-db-only**] [**cos** *cos-no*] [**ttl** *ttl*] [**detail**]

Syntax Description

domain *domain-name*	String of a maximum of 80 characters that identifies the domain in which the destination MEP resides. (Basic traceroute)
service *service-name*	String of a maximum of 80 characters that identifies the maintenance association to which the destination MEP belongs. (Basic traceroute)
mac-address *target-mac-address*	Identifies the 6-byte MAC address (in hexadecimal H.H.H format) of the destination MEP. (Targeted traceroute)
mep-id *target-mepid*	Destination maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191. (Targeted traceroute)
explore	(Optional) Specifies that an exploratory traceroute is performed.
all-ports	(Optional) Specifies an exploratory traceroute of all ports.
from *from-mac-address*	(Optional) Specifies an exploratory traceroute beginning at the specified MAC address (in hexadecimal H.H.H format).
source	Specifies source information for the traceroute.
mep-id *source-mep-id*	(Optional) Source maintenance end point (MEP) ID number. The range for MEP ID numbers is 1 to 8191.
interface *type*	Source interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
asynchronous	(Optional) Specifies that the traceroute is performed asynchronously, where control is returned to the command prompt immediately, and no results are displayed. The results can be displayed later using the **show ethernet cfm traceroute-cache** command.

timeout *seconds*	(Optional) Timeout value (in seconds) for the specified interface. For a basic traceroute, the timeout is a fixed value that defaults to 5 seconds. For an exploratory traceroute, a logarithmic algorithm is used unless this value is specified.
filtering-db-only	(Optional) Sets whether or not the remote maintenance points should base their responses on the filtering database only. The default is no—use both the filtering and MIP-CCM databases. **Note** The **filtering-db-only** option is only available for basic traceroute (when the MAC address or MEP ID is specified). It is not available with the **explore** option.
cos *cos-no*	(Optional) Identifies the class of traffic of the source MEP by setting a Class of Service (CoS) value. The valid values are from 0 to 7.
ttl *ttl*	Specifies the initial time-to-live (TTL) value (from 1 to 255) for the traceroute message. The default is 64.
detail	(Optional) Specifies that details are displayed in the output for the traceroute.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

By default, this command pauses until the traceroute operation is complete, then displays the results. If the **asynchronous** option is used, this command returns immediately and no results are displayed. Results are placed placed the traceroute cache and can be retrieved using the **show ethernet cfm traceroute-cache** command.

An exploratory traceroute, by default uses a **timeout** value that is calculated by a logarithmic delay algorithm. If the **timeout** value is specified, the specified value is used.

The display output of this command is similar to the output of the **show ethernet cfm traceroute-cache** command.

Task ID

Task ID	Operations
interface	read

Examples

The following example shows how generate a basic traceroute:

```
RP/0/RP0:hostname# traceroute ethernet cfm domain bar service bar mep-id 1 source interface
 TenGigE0/0/0/0

Traceroutes in domain bar (level 4), service bar
Source: MEP-ID 1, interface TenGigE0/0/0/0
```

```
================================================================================
Traceroute at 2009-05-18 12:09:10 to 0001.0203.0402,
TTL 64, Trans ID 2:

Hop Hostname/Last            Ingress MAC/name       Egress MAC/Name        Relay
--- ------------------------ ---------------------- ---------------------- -----
  1 ios                      0001.0203.0400 [Down]                         FDB
      0000-0001.0203.0400    Te0/0/0/0
  2 abc                                             0001.0203.0401 [Ok]    FDB
      ios                                           Not present
  3 bcd                      0001.0203.0402 [Ok]                           Hit
      abc                    Te0/0
Replies dropped: 0
```

uni-directional link-fault detection

To enable detection of a local, unidirectional link fault and send notification of that fault to an Ethernet OAM peer, use the **uni-directional link-fault detection** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode. To remove the configuration from a profile and return to the default, or to remove the override configuration at an interface, use the **no** form of this command.

uni-directional link-fault detection [**disable**]
no uni-directional link-fault detection [**disable**]

Syntax Description

disable	(Optional, Interface Ethernet OAM configuration only) Overrides the setting of unidirectional link fault detection from an Ethernet OAM profile, and disables it for this interface only.

Command Default

Detection and sending notification of local, unidirectional link faults is disabled.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

This command does not affect how the receipt of link-fault messages are handled by the router. Actions to be taken for the receipt of link-fault messages are configured using the **action uni-directional link-fault** command.

Consider the following guidelines when configuring the **uni-directional link-fault detection** command:

- You can configure unidirectional link-fault detection for multiple interfaces that share a similar configuration using the command within an Ethernet OAM profile and attaching the profile to the interfaces to which it applies.
- You can override the profile configuration for unidirectional link-fault detection using the command in interface Ethernet OAM configuration.
- The **disable** keyword is only available in interface Ethernet OAM configuration mode, and it allows you to override the feature set by the profile, and disable it for a particular interface. For example, if unidirectional link-fault detection is enabled within a profile that is attached to an interface, you can override that configuration to disable it at the interface using the **uni-directional link-fault detection disable** command in interface Ethernet OAM configuration mode.
- You can use the **no** form of the command in either the profile or interface configuration:
  - Running the **no** form of the command within the profile removes the configuration of the uni-directional command in the profile, effectively disabling the feature for all interfaces.
  - Running the **no** form of the command within interface Ethernet OAM configuration removes the override setting of the command at the interface and uses the profile setting.
- The **show ethernet oam configuration** command output will show either Y or N and (Overridden) depending on whether the interface is driving the configuration of the feature, or the profile is driving it. “Overriden” means that the configuration is being applied by the interface.

Task ID

Task ID	Operations
ethernet-services	read, write

Examples

The following example shows how to enable detection of a local, unidirectional link fault and send notification of that fault to an Ethernet OAM peer within an Ethernet OAM profile that can be attached to multiple interfaces:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
RP/0/RP0:hostname(config-eoam)# uni-directional link-fault detection
```

The same profile can be applied to multiple interfaces. The following example shows how to attach the Ethernet OAM profile to an interface:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# profile Profile_1
RP/0/RP0:hostname(config-if-eoam)# commit
```

Consider that you have decided that you do not want unidirectional link-fault detection enabled at this particular interface, but you do want to keep the other attached profile settings. The following example shows how to disable link-fault detection at this interface only:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet oam
RP/0/RP0:hostname(config-if-eoam)# uni-directional link-fault detection disable
RP/0/RP0:hostname(config-if-eoam)# commit
```

fault oam

The **fault oam** command triggers fault OAM messages which are used to communicate faults at server layer MEP to the client layer MEP.

fault oam

no fault oam

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Bidirectional Interface Configuration Mode

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to use the **fault oam** command:

```
RP0/0/0/CPU0: router (config-if-bidir) # fault oam
```

mpls-oam

To enable MPLS OAM LSP verification, use the **mpls-oam** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

mpls-oam

no mpls-oam

Syntax Description

This command has no keywords or arguments.

Command Default

By default, MPLS OAM is disabled.

Command Modes

Global Configuration

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read, write

Example

The following example shows how to use the **mpls-oam** command:

```
RP/0/RP0: router (config) # mpls-oam
```

path-option (MPLS-TE)

To configure a path option for an MPLS-TE tunnel, use the **path-option** command in tunnel-te interface configuration mode. To return to the default behavior, use the **no** form of this command.

path-option *preference-priority* [**protecting** *number*] { **dynamic** [**pce** [**address ipv4** *address*]] | **explicit** { **name** *path-name* | **identifier** *path-number* } [**protected-by** *path-option-level*] } **[attribute-set** *name]* [**isis** *instance-name* **level** *level*] [**lockdown**] [**sticky**] [**ospf** *instance-name* **area** { *value address* }] [**verbatim**]
no path-option *preference-priority* {**dynamic** [**pce** [**address ipv4** *address*]] | **explicit** {**name** *path-name* | **identifier** *path-number*}[**protected-by** *path-option-level*]} [**isis** *instance-name* **level** *level*] [**lockdown**] [**ospf** *instance-name* **area** {*value address*}] [**verbatim**]

Syntax Description

preference-priority	Path option number. Range is from 1 to 1000.
protecting *number*	Specifies a path setup option to protect a path. The range is from 1 to 1000.
dynamic	Specifies that label switched paths (LSP) are dynamically calculated.
pce	(Optional) Specifies that the LSP is computed by a Path Computation Element (PCE).
address	(Optional) Configures the address for the PCE.
ipv4 *address*	Configures the IPv4 address for the PCE.
explicit	Specifies that LSP paths are IP explicit paths.
name *path-name*	Specifies the path name of the IP explicit path.
identifier *path-number*	Specifies a path number of the IP explicit path.
protected-by *path-option-level*	(Optional) Configures path protection for an explicit path that is protected by another explicit path.
isis *instance-name*	(Optional) Limits CSPF to a single IS-IS instance and area.
attribute-set *name*	(Optional) Specifies the attribute set for the LSP.
level *level*	Configures the level for IS-IS. The range is from 1 to 2.
lockdown	(Optional) Specifies that the LSP cannot be reoptimized.
sticky	(Optional) Extended version of lockdown. LSP stays on the same path after change in resources. **Note** The sticky option can be configured only on the primary path option.
ospf *instance-name*	(Optional) Limits CSPF to a single OSPF instance and area.
area	Configures the area for OSPF.

value	Decimal value for the OSPF area ID.
address	IP address for the OSPF area ID.
verbatim	(Optional) Bypasses the Topology/CSPF check for explicit paths.

Command Default

No default behavior or values

Command Modes

Tunnel-te interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

You can configure several path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. The path setup preference is for lower (not higher) numbers, so option 1 is preferred.

When the lower number path option fails, the next path option is used to set up a tunnel automatically (unless using the lockdown option).

The **protecting** keyword specifies that you can configure path-protection for the primary LSP. The **protecting** keyword is available only for tunnel-gte interfaces.

You specify the backup path for the **path-option** command in case of the primary path failure.

CSPF areas are configured on a per-path-option basis.

The **dynamic** keyword is required to configure path-protection.

Any primary explicit path on a path protection enabled tunnel can be configured to be protected by an explicit path option level using **protected-by** keyword. Only one explicit protecting path is supported per path option.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure the tunnel to use a named IPv4 explicit path as verbatim and lockdown options for the tunnel. This tunnel cannot reoptimize when the FRR event goes away, unless you manually reoptimize it:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 explicit name test verbatim lockdown
```

The following example shows how to enable path protection on a tunnel to configure an explicit path:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 explicit name po4
```

```
RP/0/RP0:hostname(config-if)# path-option protecting 1 explicit name po6
```

The following example shows how to limit CSPF to a single OSPF instance and area:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 explicit name router1 ospf 3 area 7 verbatim
```

The following example shows how to limit CSPF to a single IS-IS instance and area:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 dynamic isis mtbf level 1 lockdown
```

mpls traffic-eng path-protection switchover

To force a manual switchover for path-protected tunnel, use the **mpls traffic-eng path-protection switchover** command in EXEC mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng path-protection switchover [**non-revertive**] **tunnel** *tunnel_name*
no mpls traffic-eng path-protection switchover [**non-revertive**] **tunnel** *tunnel_name*

Syntax Description

non-revertive	(Optional) Configures the LSP to not switch back to the original working path.
tunnel *tunnel_name*	Switchover occurs for the specified tunnel name.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read, write

Example

This example shows how to use the **mpls traffic-eng path-protection switchover** command:

```
RP/0/RP0:router# mpls traffic-eng path-protection switchover non-revertive tunnel t1
```

mpls traffic-eng reroute

To configure the router to assign new or more efficient backup MPLS-TE tunnels and to clear sticky paths for protected MPLS-TE tunnels, use the **mpls traffic-eng reroute** command in EXEC mode. To return to the default behavior, use the **no** form of this command.

mpls traffic-eng reroute tunnel *tunnel_name*
no mpls traffic-eng reroute tunnel *tunnel_name*

Syntax Description

tunnel *tunnel_name*	Clears sticky paths for the specified tunnel.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.29	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read, write

Example

This example shows how to use the **mpls traffic-eng reroute** command:

```
RP/0/RP0: router # mpls traffic-eng reroute tunnel t1
```

VPWS Command Reference

This chapter describes the commands to configure VPWS.

discovery targeted-hello

To configure the interval between transmission of consecutive Label Distribution Protocol (LDP) discovery targeted-hello messages, the hold time for a discovered targeted LDP neighbor, and to accept targeted hello from peers, use the **discovery targeted-hello** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

discovery targeted-hello address-family { } { **accept** | | **holdtime** *seconds* | **interval** *seconds* }

no discovery targeted-hello { } { **accept** | | **holdtime** *seconds* | **interval** *seconds* }

Syntax Description

accept	Accepts targeted hellos from any source.
holdtime	Configures the time a discovered LDP neighbor is remembered without receipt of an LDP hello message from a neighbor.
interval	Displays time between consecutive hello messages.
seconds	Time value, in seconds. Range is 1 to 65535.

Command Default

accept: Targeted hello messages are not accepted from any source (neighbor).

holdtime: 90

interval: 10

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

The following example shows how to configure the targeted-hello holdtime to 45 seconds, interval to 5 seconds, and configure acceptance of targeted hellos from all peers:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls ldp
RP/0/RP0:hostname(config-ldp)# discovery targeted-hello holdtime 45
RP/0/RP0:hostname(config-ldp)# discovery targeted-hello interval 5
RP/0/RP0:hostname(config-ldp)# discovery targeted-hello accept
```

graceful-restart

To configure graceful restart, use the **graceful-restart** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

graceful-restart [**reconnect-timeout** *seconds* | **forwarding-state-holdtime** *seconds*]

no graceful-restart [**reconnect-timeout** *seconds* | **forwarding-state-holdtime** *seconds*]

Syntax Description

reconnect-timeout *seconds*	(Optional) Configures the time that the local LDP sends to its graceful restartable peer, indicating how long its neighbor should wait for reconnection in the event of a LDP session failure, in seconds. Range is 60 to 1800
forwarding-state-holdtime *seconds*	(Optional) Configures the time the local forwarding state is preserved (without being reclaimed) after the local LDP control plane restarts, in seconds. Range is 60 to 1800.

Command Default

By default, graceful restart is disabled.

reconnect-timeout: 120

forwarding-state-holdtime : 180

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the LDP graceful restart capability to achieve nonstop forwarding (NSF) during an LDP control plane communication failure or restart. To configure graceful restart between two peers, enable LDP graceful restart on both label switch routers (LSRs).

When an LDP graceful restart session is established and there is control plane failure, the peer LSR starts graceful restart procedures, initially keeps the forwarding state information pertaining to the restarting peer, and marks this state as stale. If the restarting peer does not reconnect within the reconnect timeout, the stale forwarding state is removed. If the restarting peer reconnects within the reconnect time period, it is provided recovery time to resynchronize with its peer. After this time, any unsynchronized state is removed.

The value of the forwarding state hold time keeps the forwarding plane state associated with the LDP control-plane in case of a control-plane restart or failure. If the control plane fails, the forwarding plane retains the LDP forwarding state for twice the forwarding state hold time. The value of the forwarding state hold time is also used to start the local LDP forwarding state hold timer after the LDP control plane restarts. When the LDP graceful restart sessions are renegotiated with its peers, the restarting LSR sends the remaining value

of this timer as the recovery time to its peers. Upon local LDP restart with graceful restart enabled, LDP does not replay forwarding updates to MPLS forwarding until the forwarding state hold timer expires.

Note In the presence of a peer relationship, any change to the LDP graceful restart configuration will restart LDP sessions. If LDP configuration changes from nongraceful restart to graceful restart, all the sessions are restarted. Only graceful restart sessions are restarted upon graceful restart to nongraceful restart configuration changes.

Task ID

Task ID	Operations
mpls-ldp	read, write

The following example shows how to configure an existing session for graceful restart:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls ldp
RP/0/RP0:hostname(config-ldp)# graceful-restart
```

interface

To configure an attachment circuit, use the **interface** command in p2p configuration submode. To return to the default behavior, use the **no** form of this command.

interface *type interface path-id* [**PW-Ether**]

no interface *type interface path-id* [**PW-Ether**]

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
PW-Ether	(Optional) Configures an Ethernet Interface.

Command Default

None

Command Modes

p2p configuration submode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how to configure an attachment circuit on a TenGigE interface:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group group1
RP/0/RP0:hostname(config-l2vpn-xc)# p2p xc1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface TenGigE 0/3/0/11
```

ipv4 source

To configure source IP address for the pseudowire class with encapsulation mpls, use the **ipv4 source** command in the L2VPN pseudowire class encapsulation mpls configuration mode.

ipv4 source *source-ip-address*

Syntax Description

source-ip-address	Source IP address

Command Default

None

Command Modes

L2VPN pseudowire class encapsulation mpls configuration.

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

This example shows how to configure the source IP address:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
 RP/0/RP0:hostname(config-l2vpn)# pw-class kant1
RP/0/RP0:hostname(config-l2vpn-pwc)# encapsulation mpls
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)# ipv4 source 112.22.1.4
```

log neighbor

To enable logging of notices describing session changes, use the **log neighbor** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

log neighbor

no log neighbor

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **log neighbor** command to receive a syslog or console message when a neighbor goes up or down.

Task ID

Task ID	Operations
mpls-ldp	read, write

The following example shows how to enable logging messages for neighbor session up and down events:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls ldp
RP/0/RP0:hostname(config-ldp)# log neighbor
```

A logging message is issued when an LDP session state changes from up to down (and down to up).

l2vpn

To enter L2VPN configuration mode, use the **l2vpn** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

l2vpn

no l2vpn

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note All L2VPN configuration can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how to enter L2VPN configuration mode:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)#
```

l2 transport propagate

To propagate Layer 2 transport events, use the **l2transport propagate** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

l2transport propagate remote-status

no l2transport propagate remote-status

Syntax Description

remote-status	Propagates remote link status changes.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **l2transport propagate** command provides a mechanism for the detection and propagation of remote link failure for port mode VPWS.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how to propagate remote link status changes:

```
RP/0/RP0:hostname# configure
 RP/0/RP0:hostname(config)# interface TenGigE0/3/0/11
 RP/0/RP0:hostname(config-if)# l2transport propagate remote-status
```

load-balancing flow-label

To balance the load based on flow-labels, use the **load-balancing flow label** command in the l2vpn pseudowire class mpls configuration submode. To undo flow-label based load-balancing, use the **no** form of this command.

load-balancing flow-label both

Syntax Description

both	Inserts or discards flow labels on transmit or receive.

Command Default

None

Command Modes

L2vpn pseudowire class mpls configuration submode

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
l2vpn	read, write

Example

The following example shows how to configure flow labels.

```
RP/0/RP0:hostname # configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# pw-class kanata01
 RP/0/RP0:hostname(config-l2vpn-pwc)# encapsulation mpls
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)# protocol ldp
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)#transport-mode ethernet
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)#load-balancing
RP/0/RP0:hostname(config-l2vpn-pwc-mpls-load-bal)#flow-label both
RP/0/RP0:hostname(config-l2vpn-pwc-mpls-load-bal)#!
RP/0/RP0:hostname(config-l2vpn-pwc-mpls-load-bal)#commit
```

mpls ldp

To enter MPLS Label Distribution Protocol (LDP) configuration mode, use the **mpls ldp** command in global configuration mode.

mpls ldp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

The following example shows how to MPLS LDP configuration mode:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls ldp
RP/0/RP0:hostname(config-ldp)#
```

mpls static label

To configure static labels for MPLS L2VPN, use the **mpls static label** command in L2VPN cross-connect P2P pseudowire configuration mode. To have MPLS assign a label dynamically, use the **no** form of this command.

mpls static label local *label* **remote** *value*

no mpls static label local *label* **remote** *value*

Syntax Description

local *label*	Configures a local pseudowire label. Range is 16 to 15999.
remote *value*	Configures a remote pseudowire label. Range is 16 to 15999.

Command Default

The default behavior is a dynamic label assignment.

Command Modes

L2VPN cross-connect P2P pseudowire configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how to configure static labels for MPLS L2VPN:

```
 RP/0/RP0:hostname# configure
 RP/0/RP0:hostname(config)# l2vpn
 RP/0/RP0:hostname(config-l2vpn)# xconnect group group1
 RP/0/RP0:hostname(config-l2vpn-xc)# p2p xc1
 RP/0/RP0:hostname(config-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# mpls static label local 800 remote 500
```

neighbor

To configure a pseudowire for a cross-connect, use the **neighbor** command in p2p configuration submode. To return to the default behavior, use the **no**form of this command.

neighbor { *A.B.C.D* | **ipv4** *ipv4 address* } **pw-id** *value* [**mpls** || **pw-class**]

no neighbor { *A.B.C.D* | **ipv4** *ipv4 address* } **pw-id** *value* [**mpls** || **pw-class**]

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note All L2VPN configurations can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how to define a simple pseudowire class template:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group l1vpn
RP/0/RP0:hostname(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class kanata01
```

nsr

To configure nonstop routing for LDP protocols in the event of a disruption in service, use the **nsr** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

nsr

no nsr

Syntax Description

This command has no keywords or arguments.

Command Default

By default, MPLS LDP NSR is disabled.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A disruption in service may include any of the following events:

- Route Processor (RP) switchover
- LDP process restart
- In-service system upgrade (ISSU)

Enabling NSR causes events such as these to be invisible to the routing peers and provide minimal service disruption.

Note The LDP Process restart is supported by NSR only if the NSR process-failures switchover is configured, else the process restart causes the session to be unstable.

Task ID

Task ID	Operations
mpls-ldp	read, write

The following example shows how to enable MPLS LDP NSR:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls ldp
RP/0/RP0:hostname(config-ldp)# nsr
```

preferred path

To configure an MPLS TE tunnel to be used for L2VPN traffic, use the **preferred-path** command in Encapsulation MPLS configuration mode. To delete the preferred-path, use the **no** form of this command.

preferred-path interface { **tunnel-te** } *value* [**fallback disable**]

no preferred-path interface { **tunnel-te** } *value* [**fallback disable**]

Syntax Description

interface	Interface for the preferred path.
value	IP tunnel interface name for the preferred path.
fallback disable	(Optional) Disables fallback for preferred path tunnel settings.
tunnel-te	Specifies the TE tunnel interface name for the preferred path.

Command Default

None

Command Modes

l2vpn pseudowire class mpls encapsulation mode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **preferred-path** command is applicable only to pseudowires with MPLS encapsulation.

Use the show l2vpn xconnect detail command to show the status of fallback (that is, enabled or disabled).

Note All L2VPN configurations can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

This example shows how to configure preferred-path tunnel settings:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class kanata01
RP/0/RP0:hostname(config-l2vpn-pwc)# encapsulation mpls
RP/0/RP0:hostname(config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te 345
RP/0/RP0:hostname(config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te 345
fallback disable
```

pw-class

To enter pseudowire class submode to define a pseudowire class template, use the **pw-class** command in L2VPN configuration submode. To delete the pseudowire class, use the **no** form of this command.

pw-class *class-name*

no pw-class *class-name*

Syntax Description

class-name	Pseudowire class name.

Command Default

None

Command Modes

L2VPN configuration submode

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note All L2VPN configurations can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how to define a simple pseudowire class template:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group l1vpn
RP/0/RP0:hostname(config-l2vpn-xc)# p2p rtrA_to_rtrB
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class kanata01
```

pw-class encapsulation mpls

To configure MPLS pseudowire encapsulation, use the **pw-class encapsulation mpls** command in L2VPN pseudowire class configuration mode. To undo the configuration, use the **no** form of this command.

pw-class *class-name* **encapsulation mpls** { **ipv4** | **preferred-path** | **protocol ldp** | **transport-mode** }

no pw-class *class-name* **encapsulation mpls** { **ipv4** | **preferred-path** | **protocol ldp** | **transport-mode** }

Syntax Description

class-name	Encapsulation class name
ipv4	Sets the local source IPv4 address.
preferred-path	(Optional) Configures the preferred path tunnel settings.
protocol ldp	Configures LDP as the signaling protocol for this pseudowire class.
transport-mode	(Optional) Configures transport mode to Ethernet.

Command Default

None

Command Modes

L2VPN pseudowire class configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note All L2VPN configurations can be deleted using the **no l2vpn** command.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows a point-to-point cross-connect configuration :

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# pw-class kanata01
RP/0/RP0:hostname (config-l2vpn-pwc)# encapsulation mpls
```

```
RP/0/RP0:hostname (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RP0:hostname (config-l2vpn-pwc-encap-mpls)# ipv4 source 1.1.1.1
RP/0/RP0:hostname (config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te 1
```

pw load-balance terminated

Use the **fat-pw load-balance terminated** command to configure the ingress interface of the egress PE node so that LAG hashing is performed using the terminating header of the traffic that is received.

Prior to R6.5.31, FAT pseudowire load balancing is supported for LAG NNI interface with insertion upto three labels. From R6.5.31 onwards, FAT-PW load balancing is supported for LAG NNI interface with insertion upto five labels.

fat-pw load-balance terminated

Syntax Description

fat-pw	Configures the fat pseudo wire profile on the interface
load-balance	load balance type
terminated	load balance on terminated header

Command Default

None

Command Modes

config mode

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure flow labels.

```
RP/0/RP0:hostname # configure
RP/0/RP0:hostname(config)# int FortyGigE0/0/0/2
RP/0/RP0:hostname(config-if)# fat-pw load-balance terminated
 RP/0/RP0:hostname (config-if)# commit
```

p2p

To enter p2p configuration submode to configure point-to-point cross-connects, use the **p2p** command in L2VPN xconnect mode. To return to the default behavior, use the **no** form of this command.

p2p *xconnect-name*

no p2p *xconnect-name*

Syntax Description

xconnect-name	(Optional) Configures the name of the point-to-point cross- connect.

Command Default

None

Command Modes

L2VPN xconnect

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The name of the point-to-point cross-connect string is a free format description string.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows a point-to-point cross-connect configuration:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group group1
RP/0/RP0:hostname(config-l2vpn-xc)# p2p xc1
```

router-id

To specify an IPv4 address to act as the router ID, use the **router-id** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

router-id *lsr-id*

no router-id *lsr-id*

Syntax Description

lsr-id	LSR ID in A.B.C.D format.

Command Default

LDP uses router ID as determined by global router ID agent, IP Address Repository Manager (IP ARM).

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

LDP uses the router ID from different sources in the following order:

1. Configured LDP router ID.
2. Global router ID (if configured).
3. Calculated (computed) using the primary IPv4 address of the highest numbered configured loopback address. We recommend configuring at least one loopback address.

Note We recommend that you configure an IP address for the LDP router-id to avoid unnecessary session flaps.

Task ID

Task ID	Operations
mpls-ldp	read, write

We recommend that you configure an IP address for the LDP router-id to avoid unnecessary session flaps.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls ldp
RP/0/RP0:hostname(config-ldp)# router-id 10.0.0.1
```

session protection

To enable the LDP session protection feature for keeping LDP peer session up by means of targeted discovery following the loss of link discovery with a peer, use the **session protection** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

session protection [**duration** *seconds* | **infinite**]

no session protection

Syntax Description

duration *seconds*	(Optional) Specifies the protection duration, that is, the number of seconds that targeted discovery should continue following the loss of link discovery to a neighbor. Range is 30 to 2147483.
infinite	(Optional) Specifies session protection to last forever after loss of link discovery.

Command Default

By default, session protection is disabled. When enabled without duration, session protection is provided for all LDP peers and continues for 24 hours after a link discovery loss.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

LDP session protection feature allows you to enable the automatic setup of targeted hello adjacencies with all or a set of peers and specify the duration for which session needs to be maintained using targeted hellos after loss of link discovery.

Task ID

Task ID	Operations
mpls-ldp	read, write

The following example shows how to enable session protection for all discovered peers with unlimited duration to maintain the session after link discovery loss:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls ldp
RP/0/RP0:hostname(config-ldp)# session protection
```

xconnect group

To configure cross-connect groups, use the **xconnect group** command in L2VPN configuration mode. To return to the default behavior, use the **no** form of this command.

xconnect group *group-name*

no xconnect group *group-name*

Syntax Description

group-name	Configures a cross-connect group name using a free-format 32-character string.

Command Default

None

Command Modes

L2VPN configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note You can configure up to a maximum of 16K cross-connects per box.

Task ID

Task ID	Operations
l2vpn	read, write

The following example shows how to group all cross -connects for customer_atlantic:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group customer_atlantic
```

BGP Route Reflector Commands

This chapter provides details of the commands used for configuring Border Gateway Protocol (BGP) Route Reflector (RR).

address-family (BGP)

To enter various address family configuration modes while configuring Border Gateway Protocol (BGP), use the **address-family** command in an appropriate configuration mode. To disable support for an address family, use the **no** form of this command.

address-family { **ipv4 unicast** | **ipv4 multicast** | **ipv4 labeled-unicast** | **ipv4 tunnel** | **vpnv4 unicast** }
no address-family { **ipv4 unicast** | **ipv4 multicast** | **ipv4 labeled-unicast** | **ipv4 tunnel** | **vpnv4 unicast** }

Syntax Description

ipv4 unicast	Specifies IP Version 4 (IPv4) unicast address prefixes.
ipv4 multicast	Specifies IPv4 multicast address prefixes.
ipv4 labeled-unicast	Specifies IPv4 labeled-unicast address prefixes. This option is available in IPv4 neighbor configuration mode and VRF neighbor configuration mode.
ipv4 tunnel	Specifies IPv4 tunnel address prefixes.
vpnv4 unicast	Specifies VPN Version 4 (VPNv4) unicast address prefixes. This option is not available in VRF or VRF neighbor configuration mode.

Command Default

An address family must be explicitly configured in the router configuration mode for the address family to be active in BGP. Similarly, an address family must be configured under the neighbor for the BGP session to be established for that address family. An address family must be configured in router configuration mode before it can be configured under a neighbor.

Command Modes

Router configuration

Neighbor configuration

Neighbor group configuration

VRF configuration

VRF neighbor configuration (IPv4 address families)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **address-family** command to enter various address family configuration modes while configuring BGP routing sessions. When you enter the **address-family** command from router configuration mode, you enable the address family and enter global address family configuration mode.

The IPv4 unicast address family must be configured in router configuration mode before configuring the IPv4 labeled-unicast address family for a neighbor in neighbor configuration mode.

Table 73: Address Family Submode Support

Address Family	Supported in Router Submode	Supported in Neighbor Submode	Comments
ipv4 unicast	Yes	Yes	-
ipv4 multicast	Yes	Yes	-
ipv4 tunnel	Yes	Yes	-
ipv4 labeled-unicast	Yes	Yes	The ipv4 labeled-unicast address family can be configured only as a neighbor address family;however, the ipv4 unicast address family must be configured as the router address family first.
vpnv4 unicast	Yes	Yes	-

When you enter the **address-family** command from neighbor configuration mode, you activate the address family on the neighbor and enter neighbor address family configuration mode.

IPv4 neighbor sessions support IPv4 unicast, multicast, labeled-unicast, and VPNv4 unicast address families.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to place the router in global address family configuration mode for the IPv4 address family:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router bgp 100
RP/0/RP0:hostname(config-bgp)# address-family ipv4 unicast
RP/0/RP0:hostname(config-bgp-af)#
```

The following example shows how to activate IPv4 multicast for neighbor 10.0.0.1 and place the router in neighbor address family configuration mode for the IPv4 multicast address family:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname# router bgp 1
RP/0/RP0:hostname(config-bgp)# address-family ipv4 multicast
RP/0/RP0:hostname(config-bgp-af)# exit
RP/0/RP0:hostname(config-bgp)# neighbor 10.0.0.1
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 1
RP/0/RP0:hostname(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0:hostname(config-bgp-nbr-af)#
```

additional-paths selection

To configure additional paths selection mode for a prefix, use the **additional-paths selection** command in the appropriate configuration mode. Use the **additional-paths selection** command with an appropriate route-policy to calculate backup paths and to enable Prefix Independent Convergence (PIC) functionality.

additional-paths selection route-policy *route-policy name*

Syntax Description

route-policy *route-policy name*	Specifies the name of a route policy used for additional paths selection.

Command Default

None

Command Modes

IPv4 address family configuration

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Usage Guidelines

To configure additional paths selection mode for some or all prefixes, use the **additional-paths selection** command by specifying a route-policy.

Example

The following example shows how to use the **additional-paths selection** command:

```
RP/0/RP0:hostname (config-bgp-af)# additional-paths selection route-policy a1
```

keychain

To apply key chain-based authentication on a TCP connection between two Border Gateway Protocol (BGP) neighbors, use the **keychain** command in an appropriate configuration mode. To disable key chain authentication, use the **no** form of this command.

keychain *name*
no keychain [{*name*}]

Syntax Description

name	Key chain name configured using the **keychain** command. The name must be a maximum of 32 alphanumeric characters.

Command Default

When this command is not specified in the appropriate configuration mode, key chain authentication is not enabled on a TCP connection between two BGP neighbors.

Command Modes

Neighbor configuration

Neighbor group configuration

Session group configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Specify a key chain to enable key chain authentication between two BGP peers. Use the **keychain** command to implement hitless key rollover for authentication.

If this command is configured for a neighbor group or a session group, a neighbor using the group inherits the configuration. Values of commands configured specifically for a neighbor override inherited values.

Note BGP only supports HMAC-MD5 and HMAC-SHA1-12 cryptographic algorithms.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure neighbor 172.20.1.1 to use the key chain authentication configured in the keychain_A key chain:

```
RP/0/RP0:hostname(config)# router bgp 140
RP/0/RP0:hostname(config-bgp)# neighbor 172.20.1.1
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 1
RP/0/RP0:hostname(config-bgp-nbr)# keychain keychain_A
```

neighbor (BGP)

To enter neighbor configuration mode for configuring Border Gateway Protocol (BGP) routing sessions, use the **neighbor** command in an appropriate configuration mode. To delete all configuration for a neighbor and terminate peering sessions with the neighbor, use the **no** form of this command.

neighbor *ip-address*
no neighbor *ip-address*

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to place the router in neighbor configuration mode for BGP routing process 1 and configure the neighbor IP address 172.168.40.24 as a BGP peer:

```
RP/0/RP0:hostname(config)# router bgp 1
RP/0/RP0:hostname(config-bgp)# neighbor 172.168.40.24
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 65000
```

remote-as (BGP)

To create a Border Gateway Protocol (BGP) neighbor and begin the exchange of routing information, use the **remote-as** command in an appropriate configuration mode. To delete the entry for the BGP neighbor, use the **no** form of this command.

remote-as *as-number*
no remote-as [*as-number*]

Syntax Description

as-number Autonomous system (AS) to which the neighbor belongs.

- Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535.
- Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295.
- Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535.

Command Default

No BGP neighbors exist.

Command Modes

Neighbor configuration

VRF neighbor configuration

Neighbor group configuration

Session group configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **remote-as** command to create a neighbor and assign it a remote autonomous system number. A neighbor must have a remote autonomous system number before any other commands can be configured for it. Removing the remote autonomous system from a neighbor causes the neighbor to be deleted. You cannot remove the autonomous system number if the neighbor has other configuration.

Note We recommend that you use the **no neighbor** command rather than the **no remote-as** command to delete a neighbor.

A neighbor specified with a remote autonomous system number that matches the autonomous system number specified in the **router bgp** command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

Configuration of the **remote-as** command for a neighbor group or session group using the **neighbor-group** command or **session-group** command causes all neighbors using the group to inherit the characteristics configured with the command. Configuring the command directly for the neighbor overrides the value inherited from the group.

In the neighbor configuration submode, configuring use of a session group or neighbor group for which **remote-as** is configured creates a neighbor and assigns it an autonomous system number if the neighbor has not already been created.

Note Do not combine **remote-as** commands and **no use neighbor-group** commands, or **remote-as** commands and **no use session-group** commands, in the same configuration commit.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to assign autonomous system numbers on two neighbors, neighbor 10.0.0.1, (internal) and neighbor 192.168.0.1 (external), setting up a peering session that shares routing information between this router and each of these neighbors:

```
RP/0/RP0:hostname(config)# router bgp 1
RP/0/RP0:hostname(config-bgp)# session-group group2
RP/0/RP0:hostname(config-bgp-sngrp)# remote-as 1
RP/0/RP0:hostname(config-bgp-sngrp)#exit
RP/0/RP0:hostname(config-bgp)# neighbor 10.0.0.1
RP/0/RP0:hostname(config-bgp-nbr)#use session-group group2
```

The following example shows how to configure a session group called group2 with an autonomous system number 1. Neighbor 10.0.0.1 is created when it inherits the autonomous system number 1 from session group group2.

```
RP/0/RP0:hostname(config)#router bgp 1
RP/0/RP0:hostname(config-bgp)# session-group group2
RP/0/RP0:hostname(config-bgp-sngrp)# remote-as 1
RP/0/RP0:hostname(config-bgp-sngrp)# exit
RP/0/RP0:hostname(config-bgp)# neighbor 10.0.0.1
RP/0/RP0:hostname(config-bgp-nbr)# use session-group group2
```

route-reflector-client

To configure the router as a Border Gateway Protocol (BGP) route reflector and configure the specified neighbor as its client, use the **route-reflector-client** command in an appropriate configuration mode. To disable configuring the neighbor as a client, use the **no** form of this command.

route-reflector-client [**disable**]
no route-reflector-client [**disable**]

Syntax Description

disable	(Optional) Allows the configuration inherited from a neighbor group or address family group to be overridden.

Command Default

The neighbor is not treated as a route reflector client.

Command Modes

IPv4 address family group configuration

IPv4 neighbor address family configuration

IPv4 neighbor group address family configuration

VPNv4 address family group configuration

VPNv4 neighbor address family configuration

VPNv4 neighbor group address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command is restricted to internal BGP (iBGP) neighbors only.

Use the **route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All neighbors configured with this command are members of the client group, and the remaining iBGP peers are members of the nonclient group for the local route reflector.

By default, all iBGP speakers in an autonomous system must be fully meshed with each other, and neighbors do not readvertise iBGP learned routes to other iBGP neighbors.

With route reflection, all iBGP speakers need not be fully meshed. An iBGP speaker, the route reflector, passes learned iBGP routes to some number of iBGP client neighbors. Learned iBGP routes eliminate the need for each router running BGP to communicate with every other device running BGP in the autonomous system.

The local router is a route reflector as long as it has at least one route reflector client.

If this command is configured for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows neighbor at 172.20.1.1 configured as a route reflector client for IP Version 4 (IPv4) unicast routes:

```
RP/0/RP0:hostname(config)# router bgp 140
RP/0/RP0:hostname(config-bgp)# neighbor 172.20.1.1
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 140
RP/0/RP0:hostname(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0:hostname(config-bgp-nbr-af)# route-reflector-client
```

The following example disables the route-reflector client for neighbor 172.20.1.1, preventing this feature from being automatically inherited from address family group group1:

```
RP/0/RP0:hostname(config)# router bgp 140
RP/0/RP0:hostname(config-bgp)# af-group group1 address-family ipv4 unicast
RP/0/RP0:hostname(config-bgp-afgrp)# route-reflector-client
RP/0/RP0:hostname(config-bgp-afgrp)#exit
RP/0/RP0:hostname(config-bgp)# neighbor 172.20.1.1
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 140
RP/0/RP0:hostname(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0:hostname(config-bgp-nbr-af)# use af-group group1
RP/0/RP0:hostname(config-bgp-nbr-af)# route-reflector-client inheritance-disable
```

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in config mode. To remove all BGP configurations and terminate the BGP routing process, use the **no** form of this command.

router bgp *as-number*
no router bgp [{*as-number*}]

Syntax Description

as-number Number that identifies the autonomous system (AS) in which the router resides.

- Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535.
- Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295.
- Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535.

Command Default

No BGP routing process is enabled.

Command Modes

Config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **router bgp** command to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Task ID

Task ID	Operations
bgp	read, write
rib	read, write

Examples

The following example shows how to configure a BGP process for autonomous system 120:

```
RP/0/RP0:hostname(config)# router bgp 120
```

show bgp advertised

To display advertisements for neighbors or a single neighbor, use the **show bgp advertised**command in config mode.

show bgp [**ipv4** { **unicast** | **multicast** | **labeled-unicast** | **all** | **tunnel** } | **all** { **unicast** | **multicast** | **all** | **labeled-unicast** | **tunnel** } | **vpnv4 unicast** [**rd** *rd-address*] | **vrf** { *vrf-name* | **all** } [**ipv4** { **unicast** | **labeled-unicast** }] [**rd** *rd-address*]] **advertised** [**neighbor** *ip-address*] [**summary**]

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
labeled-unicast	(Optional) Specifies labeled unicast address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
tunnel	(Optional) Specifies tunnel address prefixes.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd *rd-address*	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 { **unicast** | **labeled-unicast** }	(Optional) For VRF, specifies IPv4 unicast or labeled-unicast address families.
neighbor	(Optional) Previews advertisements for a single neighbor. If the **neighbor** keyword is omitted, then the advertisements for all neighbors are displayed.
ip-address	(Optional) IP address of the neighbor.
summary	(Optional) Displays a summary of advertisements.

Command Default

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

Config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

BGP contains a separate routing table for each address family and subaddress family combination that is configured. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp advertised** command to display the routes that have been advertised to peers or a specific peer. To preview advertisements that would be sent to a peer under a particular policy, even if the corresponding update messages have not been generated yet, use the **show bgp policy** command.

Note When you issue the **show bgp advertised** command, a route is not displayed in the output unless an advertisement for that route has already been sent (and not withdrawn). If an advertisement for the route has not yet been sent, the route is not displayed.

Use the **summary** keyword to display a summary of the advertised routes. If you do not specify the **summary** keyword, the software displays detailed information about the advertised routes.

Note The **show bgp advertised** command does not display the application of any outbound policy in the route details it displays. Consequently, this command provides only an indication of whether a particular route has been advertised, rather than details of which attributes were advertised. Use the **show bgp policy sent-advertisements** command to display the attributes that are advertised.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp advertised** command in XR EXEC mode:

```
RP/0/RP0:hostname# show bgp advertised neighbor 10.0.101.4 summary

Network     Next Hop            From          AS Path
1.1.1.0/24  10.0.101.1          10.0.101.1    2 3 222 333 444 555 i
1.1.2.0/24  10.0.101.1          10.0.101.1    3 4 5 6 7 i
1.1.3.0/24  10.0.101.1          10.0.101.1    77 88 33 44 55 99 99 99 i
1.1.4.0/24  10.0.101.1          10.0.101.1    2 5 6 7 8 i
1.1.7.0/24  10.0.101.1          10.0.101.1    3 5 i
1.1.8.0/24  10.0.101.1          10.0.101.1    77 88 99 99 99 i
```

This table describes the significant fields shown in the display.

Table 74: show bgp advertised neighbor summary Field Descriptions

Field	Description
Network	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
From	IP address of the peer that advertised this route.
AS Path	AS path of the peer that advertised this route.
Local	Indicates the route originated on the local system.
Local Aggregate	Indicates the route is an aggregate created on the local system.
Advertised to	Indicates the peer to which this entry was advertised. This field is used in the output when displaying a summary of the advertisements to all neighbors.

The following is sample output from the **show bgp advertised** command for detailed advertisement information:

```
RP/0/RP0:hostname# show bgp advertised neighbor 172.72.77.1

172.16.0.0/24 is advertised to 172.72.77.1
  Path info:
    neighbor: Local            neighbor router id: 172.74.84.1
    valid  redistributed  best
  Attributes after inbound policy was applied:
 next hop: 0.0.0.0
    MET ORG AS
    origin: incomplete  metric: 0
    aspath:
10.52.0.0/16 is advertised to 172.72.77.1
  Path info:
    neighbor: Local Aggregate  neighbor router id: 172.74.84.1
    valid  aggregated  best
  Attributes after inbound policy was applied:
 next hop: 0.0.0.0
    ORG AGG ATOM
    origin: IGP  aggregator: 172.74.84.1 (1)
    aspath:
```

This table describes the significant fields shown in the display.

Table 75: show bgp advertised neighbor Field Descriptions

Field	Description
is advertised to	IP address of the peer to which this route has been advertised. If the route has been advertised to multiple peers, the information is shown separately for each peer.

Field	Description
neighbor	IP address of the peer that advertised this route, or one of the following: Local—Route originated on the local system. Local Aggregate—Route is an aggregate created on the local system.
neighbor router id	BGP identifier for the peer, or the local system if the route originated on the local system.
Not advertised to any peer	Indicates the no-advertise well-known community is associated with this route. Routes with this community are not advertised to any BGP peers.
Not advertised to any EBGP peer	Indicates the no-export well-known community is associated with this route. Routes with this community are not advertised to external BGP peers, even if those external peers are part of the same confederation as the local router.
Not advertised outside the local AS	Indicates the local-AS well-known community is associated with this route. Routes with this community value are not advertised outside the local autonomous system or confederation boundary.
(Received from a RR-client)	Path was received from a route reflector client.
(received-only)	This path is not used for routing purposes. It is used to support soft reconfiguration, and records the path attributes before inbound policy was applied to a path received from a peer. A path marked “received-only” indicates that either the path was dropped by inbound policy, or the path information was modified by inbound policy and a separate copy of the modified path is used for routing.
(received & used)	Indicates that the path is used both for soft reconfiguration and routing purposes. A path marked “received and used,” implies the path information was not modified by inbound policy.
valid	Path is valid.
redistributed	Path is locally sourced through redistribution.
aggregated	Path is locally sourced through aggregation.
local	Path is locally sourced through the **network** command.
confed	Path was received from a confederation peer.
best	Path is selected as best.
multipath	Path is one of multiple paths selected for load-sharing purposes.

Field	Description
dampinfo	Indicates dampening information: Penalty—Current penalty for this path. Flapped—Number of times the route has flapped. In—Time (hours:minutes:seconds) since the router noticed the first flap. Reuse in—Time (hours:minutes:seconds) after which the path is made available. This field is displayed only if the path is currently suppressed.
Attributes after inbound policy was applied	Displays attributes associated with the received route, after any inbound policy has been applied. AGG—Aggregator attribute is present. AS—AS path attribute is present. ATOM—Atomic aggregate attribute is present. COMM—Communities attribute is present. EXTCOMM—Extended communities attribute is present. LOCAL—Local preference attribute is present. MET—Multi Exit Discriminator (MED) attribute is present. next hop—IP address of the next system used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network. ORG—Origin attribute is present.
origin	Origin of the path: IGP—Path originated from an Interior Gateway Protocol (IGP) and was sourced by BGP using a **network** or **aggregate-address** command. EGP—Path originated from an Exterior Gateway Protocol. incomplete—Origin of the path is not clear. For example, a route that is redistributed into BGP from an IGP.
neighbor as	First autonomous system (AS) number in the AS path.
aggregator	Indicates that the path was received with the aggregator attribute. The autonomous system number and router-id of the system that performed the aggregation are shown.
metric	Value of the interautonomous system metric, otherwise known as the MED metric.
localpref	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system
aspath	AS path associated with the route.

Field	Description
community	Community attributes associated with the path. Community values are displayed in AA:NN format, except for the following well-known communities: Local-AS—Community with value 4294967043 or hex 0xFFFFFF03. Routes with this community value are not advertised outside the local autonomous system or confederation boundary. no-advertise—Community with value 4294967042 or hex 0xFFFFFF02. Routes with this community value are not advertised to any BGP peers. no-export—Community with value 4294967041 or hex 0xFFFFFF01. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation with the local router.
Extended community	Extended community attributes associated with the path. For known extended community types, the following codes may be displayed: RT—Route target community SoO—Site of Origin community LB—Link Bandwidth community
Originator	Router ID of the originating router when route reflection is used.
Cluster lists	Router ID or cluster ID of all route reflectors through which the route has passed.

show bgp neighbors

To display information about Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp neighbors** command in config mode.

show bgp [**ipv4** { **unicast** | **multicast** | **labeled-unicast** | **all** | **tunnel** } | **all** { **unicast** | **multicast** | **all** | **labeled-unicast** | **tunnel** } | **vpnv4 unicast** | **vrf** { *vrf-name* | **all** } [**ipv4** { **unicast** | **labeled-unicast** }]] **neighbors** [**performance-statistics** | **missing-eor**]

To show one neighbor:

show bgp [**ipv4** { **unicast** | **multicast** | **labeled-unicast** | **all** | **tunnel** } | **all** { **unicast** | **multicast** | **all** | **labeled-unicast** | **tunnel** } | **vpnv4 unicast** | **vrf** { *vrf-name* | **all** } [**ipv4** { **unicast** | **labeled-unicast** }]] **neighbors** *ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **performance-statistics** | **received** { **prefix-filter** | **routes** } | **routes**]

To show default afi or safi neighbor:

show bgp neighbors ip-address [**configuration** [**defaults**] [**nvgen**] | **inheritance**]

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
labeled-unicast	(Optional) Specifies labeled unicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
tunnel	(Optional) Specifies tunnel address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 { **unicast** | **labeled-unicast** }	(Optional) For VRF, specifies IPv4 unicast or labeled-unicast address families.
performance-statistics	(Optional) Displays performance statistics relative to work done by the BGP process for this neighbor.
missing-eor	(Optional) Displays neighbors that did not send end-of-rib (EoR) notification in read-only mode.

ip-address	(Optional) IP address of the BGP-speaking neighbor. If you omit this argument, all neighbors are displayed.
advertised-routes	(Optional) Displays all routes the router advertised to the neighbor.
dampened-routes	(Optional) Displays the dampened routes that are learned from the neighbor.
flap-statistics	(Optional) Displays flap statistics of the routes learned from the neighbor.
received { **prefix-filter** | **routes** }	(Optional) Displays information received from the BGP neighbor. The options are: **prefix-filter—** Displays the prefix list filter. **routes—**Displays routes from the neighbor before inbound policy
routes	(Optional) Displays routes learned from the neighbor.
configuration	(Optional) Displays the effective configuration for the neighbor, including any settings that have been inherited from session groups, neighbor groups, or af-groups used by this neighbor.
defaults	(Optional) Displays all configuration settings, including any default settings.
nvgen	(Optional) Displays output in the **show running-config** command output.
inheritance	(Optional) Displays the session groups, neighbor groups, and af-groups from which this neighbor inherits configuration settings.
decoded-message-log	(Optional) Displays BGP message logs.
in	(Optional) Displays BGP inbound messages.
out	(Optional) Displays BGP outbound messages.
standby	Displays standby BGP information.

Command Default

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

Config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Note To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify which routing table should be examined. If the **all** keyword is specified for address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp neighbors** command to display detailed information about all neighbors or a specific neighbor. Use the **performance-statistics** keyword to display information about the work related to specific neighbors done by the BGP process.

Use the **show bgp neighbors** command with the *ip-address* **received prefix-filter** argument and keyword to display the Outbound Route Filter (ORF) received from a neighbor.

Use the **advertised-routes** keyword to display a summary of the routes advertised to the specified neighbor.

Use the **dampened-routes** keyword to display routes received from the specified neighbor that have been suppressed due to dampening. For more details, see the **show bgp dampened-paths** command.

To display information about flapping routes received from a neighbor, use the **flap-statistics** keyword. For more details, see the **show bgp flap-statistics** command.

To display the routes received from a neighbor, use the **routes** keyword. For more details, see the **show bgp** command.

Use the **show bgp neighbor** command with the *ip-address* **configuration** argument and keyword to display the effective configuration of a neighbor, including configuration inherited from session groups, neighbor groups, or af-groups through application of the **use** command. Use the **defaults** keyword to display the value of all configurations for the neighbor, including default configuration. Use the **nvgen** keyword to display configuration output format of the **show running-config** command. Output in this format is suitable for cutting and pasting into a configuration session. Use the **show bgp neighbors** command with the *ip-address* **inheritance** argument and keyword to display the session groups, neighbor groups, and af-groups from which the specified neighbor inherits configuration.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp neighbors** command:

```
RP/0/RP0:hostname# show bgp neighbors 10.0.101.1

BGP neighbor is 10.0.101.1, remote AS 2, local AS 1, external link
 Description: routem neighbor
 Remote router ID 10.0.101.1
```

```
  BGP state = Established, up for 00:00:56
  TCP open mode: passive only
BGP neighbor is 1.1.1.2
 Remote AS 300, local AS 100, external link
 Remote router ID 0.0.0.0
  BGP state = Idle (LC/FIB for the neighbor in reloading)
  Last read 00:00:00, Last read before reset 00:05:12
  Hold time is 180, keepalive interval is 60 seconds
  Configured hold time: 180, keepalive: 60, min acceptable hold time: 3

  BFD enabled (session initializing)
  Last read 00:00:55, hold time is 180, keepalive interval is 60 seconds
  DMZ-link bandwidth is 1000 Mb/s
  Neighbor capabilities:
    Route refresh: advertised
    4-byte AS: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Multicast: advertised and received
  Received 119 messages, 0 notifications, 0 in queue
  Sent 119 messages, 22 notifications, 0 in queue
  Minimum time between advertisement runs is 60 seconds

 For Address Family: IPv4 Unicast
  BGP neighbor version 137
  Update group: 1.3
  Community attribute sent to this neighbor
  AF-dependant capabilities:
    Outbound Route Filter (ORF) type (128) Prefix-list:
      Send-mode: advertised
      Receive-mode: advertised
  Route refresh request: received 0, sent 0
  Policy for incoming advertisements is pass-all
  Policy for outgoing advertisements is pass-all
  5 accepted prefixes, 5 are bestpaths
  Prefix advertised 3, suppressed 0, withdrawn 0, maximum limit 1000000
  Threshold for warning message 75%


 For Address Family: IPv4 Multicast
  BGP neighbor version 23
  Update group: 1.2
  Route refresh request: received 0, sent 0
  Policy for incoming advertisements is pass-all
  Policy for outgoing advertisements is pass-all
  2 accepted prefixes, 2 are bestpaths
  Prefix advertised 0, suppressed 0, withdrawn 0, maximum limit 131072
  Threshold for warning message 75%

  Connections established 9; dropped 8
 Last reset 00:02:10, due to User clear requested (CEASE notification sent - administrative
reset)
  Time since last notification sent to neighbor: 00:02:10
  Error Code: administrative reset
  Notification data sent:
    None
```

This table describes the significant fields shown in the display.

Table 76: show bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
Description	Neighbor specific description.
remote AS	• Number of the autonomous system to which the neighbor belongs. • Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. • Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. • Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535.
local AS	Autonomous system number of the local system. • Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. • Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. • Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535.
internal link	Neighbor is an internal BGP peer.
external link	Neighbor is an external BGP peer.
Administratively shut down	Neighbor connection is disabled using the **shutdown** command.
remote router ID	Router ID (an IP address) of the neighbor.
Neighbor under common administration	Neighbor is internal or a confederation peer.
BGP state	Internal state of this BGP connection.
BFD enabled	Status of bidirectional forwarding detection.
TCP open mode	TCP mode used in establishing the BGP session. The following valid TCP mode are supported: • default—Accept active/passive connections • passive-only—Accept only passive connections • active-only—Accept only active connections initiated by the router
Last read	Time since BGP last read a message from this neighbor.
hold time	Hold time (in seconds) used on the connection with this neighbor.
keepalive interval	Interval for sending keepalives to this neighbor.

Field	Description
DMZ-link bandwidth	DMZ link bandwidth for this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. The following valid BGP capabilities are supported: • Multi-protocol • Route refresh • Graceful restart • Outbound Route Filter (ORF) type (128) Prefix
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.
4-byte AS	Indicates that the neighbor supports the 4-byte AS capability.
Address family	Indicates that the local system supports the displayed address family capability. If "received" is displayed, the neighbor also supports the displayed address family.
Received	Number of messages received from this neighbor, the number of notification messages received and processed from this neighbor, and the number of messages that have been received, but not yet processed.
Sent	Number of messages sent to this neighbor, the number of notification messages generated to be sent to this neighbor, and the number of messages queued to be sent to this neighbor.
Minimum time between advertisement runs	Advertisement interval (in seconds) for this neighbor.
For Address Family	Information that follows is specific to the displayed address family.
BGP neighbor version	Last version of the BGP database that was sent to the neighbor for the specified address family.
Update group	Update group to which the neighbor belongs.
Route reflector client	Indicates that the local system is acting as a route reflector for this neighbor.
Inbound soft reconfiguration allowed	Indicates that soft reconfiguration is enabled for routes received from this neighbor. **Note** If the neighbor has route refresh capability, then soft configuration received-only routes are not stored by the local system unless "override route refresh" is displayed.
eBGP neighbor with no inbound or outbound policy: defaults to drop	Indicates that the neighbor does not have an inbound or outbound policy configured using the **route-policy (BGP)** command. Hence, no routes are accepted from or advertised to this neighbor.

Field	Description
Private AS number removed from updates to this neighbor	Indicates that remove-private-AS is configured on the specified address family for this neighbor.
NEXT_HOP is always this router	Indicates that next-hop-self is configured on the specified address family for this neighbor.
Community attribute sent to this neighbor	Indicates that send-community-ebgp is configured on the specified address family for this neighbor.
Extended community attribute sent to this neighbor	Indicates that send-extended-community-ebgp is configured on the specified address family for this neighbor.
Default information originate	Indicates that default-originate is configured on the specified address family for this neighbor, together with the policy used, if one was specified in the default-originate configuration. An indication of whether the default route has been advertised to the neighbor is also shown.
AF-dependant capabilities	BGP capabilities that are specific to a particular address family. The following valid AF-dependent BGP capabilities are supported: • route refresh capability • route refresh capability OLD value
Outbound Route Filter	Neighbor has the Outbound Route Filter (ORF) capability for the specified address family. Details of the capabilities supported are also shown: Send-mode—"advertised" is shown if the local system can send an outbound route filter to the neighbor. "received" is shown if the neighbor can send an outbound route filter to the local system. Receive-mode—"advertised" is shown if the local system can receive an outbound route filter from the neighbor. "received" is shown if the neighbor can receive an outbound route filter from the local system.
Graceful Restart Capability	Indicates whether graceful restart capability has been advertised to and received from the neighbor for the specified address family.
Neighbor preserved the forwarding state during latest restart	Indicates that when the neighbor connection was last established, the neighbor indicated that it preserved its forwarding state for the specified address family.
Local restart time	Restart time (in seconds) advertised to this neighbor.
RIB purge time	RIB purge time (in seconds) used for graceful restarts.
Maximum stalepath time	Maximum time (in seconds) a path received from this neighbor may be marked as stale if the neighbor restarts.
Remote Restart time	Restart time received from this neighbor.
Route refresh request	Number of route refresh requests sent and received from this neighbor.

Field	Description
Outbound Route Filter (ORF)	"sent" indicates that an outbound route filter has been sent to this neighbor. "received" indicates that an outbound route filter has been received from this neighbor. **Note** A received outbound route filter may be displayed using the **show bgp neighbors** command with the **received prefix-filter** keywords.
First update is deferred until ORF or ROUTE-REFRESH is received	If the local system advertised the receive capability and the neighbor has advertised send capability, no updates are generated until specifically asked by the neighbor (using a ROUTE-REFRESH or ORF with immediate request).
Scheduled to send the Prefix-list filter	Indicates the local system is due to send an outbound route filter request in order to receive updates from the neighbor.
Inbound path policy	Indicates if an inbound path policy is configured.
Outbound path policy	Indicates if an outbound path policy is configured.
Incoming update prefix filter list	Indicates a prefix list is configured to filter inbound updates from the neighbor.
Default weight	Default weight for routes received from the neighbor.
Policy for incoming advertisements	Indicates a route policy is configured to be applied to inbound updates from the neighbor.
Policy for outgoing advertisements	Indicates a route policy is configured to be applied to outbound updates to the neighbor.
Type	Indicates whether the condition map selects routes that should be advertised, or routes that should not be advertised: Exist—Routes advertised if permitted by the condition route map. Non-exist—Routes advertised if denied by the condition route map.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised to the neighbor during the lifetime of the current connection with the neighbor.
suppressed	Number of prefix updates that were suppressed because no transitive attributes changed from one best path to the next. **Note** Update suppression occurs only for external BGP neighbors.
withdrawn	Number of prefixes withdrawn from the neighbor during the lifetime of the current connection with the neighbor.

Field	Description
maximum limit	Maximum number of prefixes that may be received from the neighbor. If "(warning-only)" is displayed, a warning message is generated when the limit is exceeded, otherwise the neighbor connection is shut down when the limit is exceeded.
Threshold for warning message	Percentage of maximum prefix limit for the neighbor at which a warning message is generated.
Connections established	Number of times the router has established a BGP peering session with the neighbor.
dropped	Number of times that a good connection has failed or been taken down.
Last reset due to	Reason that the connection with the neighbor was last reset.
Time since last notification sent to neighbor	Amount of time since a notification message was last sent to the neighbor.
Error Code	Type of notification that was sent. The notification data, if any, is also displayed.
Time since last notification received from neighbor	Amount of time since a notification message was last received from the neighbor.
Error Code	Type of notification that was received. The notification data received, if any, is also displayed
External BGP neighbor may be up to <n> hops away	Indicates ebgp-multihop is configured for the neighbor.
External BGP neighbor not directly connected	Indicates that the neighbor is not directly attached to the local system.
Notification data sent:	Data providing more details on the error along with the error notification sent to the neighbor.

The following is sample output from the show bgp neighbors command with the advertised-routes keyword:

```
RP/0/RP0:hostname# show bgp neighbors 10.0.101.75 advertised-routes

Network Next-hop From
10.10.0.0/8 10.0.101.1 10.0.101.1
10.11.0.0/8 10.0.101.3 10.0.101.3
10.12.0.0/8 10.0.101.5 10.0.101.5
```

The following is sample output from the **show bgp neighbors** command with the **advertised-routes** keyword:

```
RP/0/RP0:hostname# show bgp neighbors 172.20.16.178 routes

BGP router identifier 172.20.16.181, local AS number 1
BGP main routing table version 27
BGP scan interval 60 secs
```

```
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network            Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         172.20.16.178        40             0 10 ?
*> 10.22.0.0        172.20.16.178        40             0 10 ?
```

The following is sample output from the **show bgp neighbors** command with the **routes** keyword:

```
RP/0/RP0:hostname# show bgp neighbors 10.0.101.1 dampened-routes

BGP router identifier 10.0.0.5, local AS number 1
BGP main routing table version 48
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            From            Reuse    Path
*d 10.0.0.0           10.0.101.1      00:59:30 2 100 1000 i
*d 11.0.0.0           10.0.101.1      00:59:30 2 100 1000 i
*d 12.0.0.0           10.0.101.1      00:59:30 2 100 1000 i
*d 13.0.0.0           10.0.101.1      00:59:30 2 100 1000 i
*d 14.0.0.0           10.0.101.1      00:59:30 2 100 1000 i
```

This table describes the significant fields shown in the display.

Table 77: show bgp neighbors routes Field Descriptions

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.

Field	Description
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** or **aggregate-address** command. e—Path originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit Discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

The following is sample output from the **show bgp neighbors** command with the **dampened-routes** keyword:

```
RP/0/RP0:hostname# show bgp neighbors 10.0.101.1 flap-statistics

BGP router identifier 10.0.0.5, local AS number 1
BGP main routing table version 48
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            From            Flaps Duration Reuse    Path
 h 10.1.0.0           10.0.101.1      5008  2d02h             2 5000 1000
 h 10.2.0.0           10.0.101.1      5008  2d02h             2 2000 3000
 h 10.2.0.0           10.0.101.1      5008  2d02h             2 9000 6000
*d 10.0.0.0           10.0.101.1      5008  2d02h    00:59:30 2 100 1000
 h 10.0.0.0/16        10.0.101.1      5008  2d02h             2 100 102
*d 10.11.0.0          10.0.101.1      5008  2d02h    00:59:30 2 100 1000
*d 10.12.0.0          10.0.101.1      5008  2d02h    00:59:30 2 100 1000
*d 10.13.0.0          10.0.101.1      5008  2d02h    00:59:30 2 100 1000
*d 10.14.0.0          10.0.101.1      5008  2d02h    00:59:30 2 100 1000
 h 192.168.0.0/16     10.0.101.1      5008  2d02h             2 100 101
```

This table describes the significant fields shown in the display.

Table 78: show bgp neighbors dampened-routes Field Descriptions

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.

Field	Description
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** or **aggregate-address** command. e—Path originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP prefix and prefix length for a network.
From	Neighbor from which the route was received.
Reuse	Time (in hours:minutes:seconds) after which the path is made available.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

The following is sample output from the **show bgp neighbors** command with the **performance-statistics** keyword:

```
RP/0/RP0:hostname# show bgp neighbors 10.0.101.2 performance-statistics

BGP neighbor is 10.0.101.2, remote AS 1
  Read 3023 messages (58639 bytes) in 3019 calls (time spent: 1.312 secs)
  Read throttled 0 times
  Processed 3023 inbound messages (time spent: 0.198 secs)
  Wrote 58410 bytes in 6062 calls (time spent: 3.041 secs)
  Processing write list: wrote 0 messages in 0 calls (time spent: 0.000 secs)
  Processing write queue: wrote 3040 messages in 3040 calls (time spent: 0.055 secs)
```

```
Received 3023 messages, 0 notifications, 0 in queue
Sent 3040 messages, 0 notifications, 0 in queue
```

This table describes the significant fields shown in the display.

Table 79: show bgp neighbors flap-statistics Field Descriptions

Field	Description
BGP route identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening has been enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between when the BGP process scans for the specified address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** command. e—Path originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP prefix and prefix length for a network.

Field	Description
From	IP address of the peer that advertised this route.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path is made available.
Path	Autonomous system path to reach the destination network.

The following is sample output from the **show bgp neighbors** command with the **configuration** keyword:

```
RP/0/RP0:hostname# show bgp neighbors 10.0.101.1 configuration

neighbor 10.0.101.1
 remote-as 2                   []
 bfd fast-detect               []
 address-family ipv4 unicast   []
  policy pass-all in           []
  policy pass-all out          []
 address-family ipv4 multicast []
  policy pass-all in           []
  policy pass-all out          []
```

This table describes the significant fields shown in the display.

Table 80: show bgp neighbors configuration Field Descriptions

Field	Description
neighbor	IP address configuration of the neighbor.
remote-as	Remote autonomous system configured on the neighbor.
bfd fast-detect	BFD parameter configured on the neighbor.
address-family	Address family and subsequent address family configured on the router.
route-policy pass-all in	Route policy configured for inbound updates.
route-policy pass-all out	Route policy configured for outbound updates.

show bgp paths

To display all the Border Gateway Protocol (BGP) paths in the database, use the **show bgp paths** command in config mode.

show bgp paths [**detail**] [**debug**] [**regexp** *regular-expression*]

Syntax Description

detail	(Optional) Displays detailed attribute information.
debug	(Optional) Displays attribute process ID, hash bucket, and hash chain ID attribute information.
regexp *regular-expression*	(Optional) Specifies an autonomous system path that matches the regular expression.

Command Default

No default behavior or values

Command Modes

Config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show bgp paths** command to display information about AS paths and the associated attributes with which the paths were received.

If no options are specified, all stored AS paths are displayed with the number of routes using each path.

Note The AS path information is stored independently of the address family, making it possible that routes from different address families could be using the same path.

Use the *regular-expression* argument to limit the output to only those paths that match the specified regular expression.

Use the **detail** keyword to display detailed information on the attributes stored with the AS path.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp paths** command:

```
RP/0/RP0:hostname# show bgp paths detail

Proc  Attributes                     Refcount    Metric Path
Spk 0 ORG AS LOCAL                          7         0 i
Spk 0 ORG AS LOCAL COMM EXTCOMM             3         0 21 i
Spk 0 MET ORG AS                            3        55 2 i
Spk 0 ORG AS                                3         0 2 10 11 i
Spk 0 ORG AS COMM                           3         0 2 10 11 i
Spk 0 MET ORG AS ATOM                       3         2 2 3 4 ?
Spk 0 MET ORG AS                            3         1 2 3 4 e
Spk 0 MET ORG AS                            3         0 2 3 4 i
```

This table describes the significant fields shown in the display.

Table 81: show bgp paths Field Descriptions

Field	Description
Proc	ID of the process in which the path is stored. This is always “Spk 0.”
Attributes	Attributes that are present. The following may appear: MET —Multi Exit Discriminator (MED) attribute is present. ORG—Origin attribute is present. AS—AS path attribute is present. LOCAL—Local preference attribute is present. AGG—Aggregator attribute is present. COMM—Communities attribute is present. ATOM—Atomic aggregate attribute is present. EXTCOMM—Extended communities attribute is present.
NeighborAS	Autonomous system number of the neighbor, or 0, if the path information originated locally. • Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. • Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. • Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535.
Refcount	Number of routes using a path.
Metric	Value of the interautonomous system metric, otherwise known as the MED metric.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** or **aggregate-address** command. e—Path originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.

show bgp policy

To display information about Border Gateway Protocol (BGP) advertisements under a proposed policy, use the **show bgp policy** command in config mode.

show bgp [**ipv4** { **unicast** | **multicast** | **labeled-unicast** | **all** | **tunnel** } | **all** { **unicast** | **multicast** | **all** | **labeled-unicast** | **tunnel** } | **vpnv4 unicast** [**rd** *rd-address*] | **vrf** { *vrf-name* | **all** } [**ipv4** { **unicast** | **labeled-unicast** }] [**rd** *rd-address*]] **policy** [**neighbor** *ip-address*] [**sent-advertisements** | **route-policy** *route-policy-name*] [**summary**]

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
labeled-unicast	(Optional) Specifies labeled unicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
tunnel	(Optional) Specifies tunnel address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd *rd-address*	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 { **unicast** | **labeled-unicast** }	(Optional) For VRF, specifies IPv4 unicast or labeled-unicast address families.
neighbor	(Optional) Previews advertisements for a single neighbor.
ip-address	(Optional) IP address of a single neighbor.
sent-advertisements	(Optional) Displays the routes that have been advertised to neighbors. If a route has not yet been advertised to the neighbor, it is not shown.
route-policy	(Optional) Displays advertisements for an output route policy.
route-policy-name	(Optional) Name of the route policy.
summary	(Optional) Displays a summary of the BGP advertisements.

Command Default

Advertisements for all neighbors are displayed if the **neighbor** *ip-address* keyword and argument are not specified. If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

Config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp policy** command to display routes that would be advertised to neighbors under a proposed policy. Unlike in the **show bgp advertised** command, the information displayed reflects any modifications made to the routes when executing the specified policy.

Use the **neighbor** keyword to limit the output to routes advertised to a particular neighbor. Use the **sent-advertisements** keyword to change the output in two ways:

- If a policy is not specified explicitly, any policy configured on the neighbor (using the **route-policy (BGP)** command) is executed before displaying the routes.
- Only routes that have already been advertised to the neighbor (and not withdrawn) are displayed. Routes that have not yet been advertised are not displayed.

Use the **summary** keyword to display abbreviated output.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp policy** command with the **summary**

```
RP/0/RP0:hostname# show bgp policy summary

Network           Next Hop        From            Advertised to
172.16.1.0/24     10.0.101.1      10.0.101.1      10.0.101.2
                                                  10.0.101.3

172.17.0.0/16     0.0.0.0         Local           10.0.101.1
                                                  10.0.101.2
```

```
                                                                10.0.101.3
```

This table describes the significant fields shown in the display.

Table 82: show bgp policy summary Field Descriptions

Field	Description
Network	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
From	IP address of the peer that advertised this route.
Local	Indicates the route originated on the local system.
Local Aggregate	Indicates the route is an aggregate created on the local system.
Advertised to	Indicates the neighbors to which this route was advertised.

The following is sample output from the **show bgp policy** command:

```
RP/0/RP0:hostname# show bgp policy

11.0.0.0/24 is advertised to 10.4.101.1
  Path info:
    neighbor: Local           neighbor router id: 10.4.0.1
    valid local best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0
    MET ORG AS
    origin: IGP metric: 0
    aspath:
  Attributes after outbound policy was applied:
    next hop: 10.4.0.1
    MET ORG AS
    origin: IGP metric: 0
    aspath: 1

11.0.0.0/24 is advertised to 10.4.101.2
  Path info:
    neighbor: Local           neighbor router id: 10.4.0.1
    valid local best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0
    MET ORG AS
    origin: IGP metric: 0
    aspath:
  Attributes after outbound policy was applied:
    next hop: 10.4.0.1
    MET ORG AS
    origin: IGP metric: 0
    aspath:

11.0.0.0/24 is advertised to 10.4.101.3
 Path info:
    neighbor: Local           neighbor router id: 10.4.0.1
```

```
    valid local best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0
    MET ORG AS
    origin: IGP metric: 0
    aspath:
  Attributes after outbound policy was applied:
    next hop: 10.4.0.1
    MET ORG AS
    origin: IGP metric: 0
    aspath:

12.0.0.0/24 is advertised to 10.4.101.2
 Path info:
    neighbor: 10.4.101.1       neighbor router id: 10.4.101.1
    valid external best
  Attributes after inbound policy was applied:
    next hop: 10.4.101.1
    ORG AS
    origin: IGP neighbor as: 2
    aspath: 2 3 4
  Attributes after outbound policy was applied:
    next hop: 10.4.101.1
    ORG AS
    origin: IGP neighbor as: 2
    aspath:2 3 4

12.0.0.0/24 is advertised to 10.4.101.3
 Path info:
    neighbor: 10.4.101.1       neighbor router id: 10.4.101.1
    valid external best
  Attributes after inbound policy was applied:
    next hop: 10.4.101.1
    ORG AS
    origin: IGP neighbor as: 2
    aspath: 2 3 4
  Attributes after outbound policy was applied:
    next hop: 10.4.101.1
    ORG AS
    origin: IGP neighbor as: 2
    aspath:2 3 4
```

This table describes the significant fields shown in the display.

Table 83: show bgp policy Field Descriptions

Field	Description
Is advertised to	IP address of the peer to which this route is advertised. If the route is advertised to multiple peers, information is shown separately for each peer.
neighbor	IP address of the peer that advertised this route, or one of the following: Local—Route originated on the local system. Local Aggregate—Route is an aggregate created on the local system.
neighbor router id	BGP identifier for the peer, or the local system if the route originated on the local system.

Field	Description
Not advertised to any peer	Indicates the no-advertise well-known community is associated with this route. Routes with this community are not advertised to any BGP peers.
Not advertised to any EBGP peer	Indicates the no-export well-known community is associated with this route. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation as the local router.
Not advertised outside the local AS	Indicates the local-AS well-known community is associated with this route. Routes with this community value are not advertised outside the local autonomous system or confederation boundary.
(Received from a RR-client)	Path was received from a route reflector client.
(received-only)	Path is not used for routing purposes. It is used to support soft reconfiguration, and records the path attributes before inbound policy was applied to a path received from a peer. A path marked "received-only" indicates that either the path was dropped by inbound policy, or that a copy of path information was created and then modified for routing use.
(received & used)	Indicates that the path is used both for soft reconfiguration and routing purposes. A path marked "(received & used)", implies the path information was not modified by inbound policy.
valid	Path is valid.
redistributed	Path is locally sourced through redistribution.
aggregated	Path is locally sourced through aggregation.
local	Path is locally sourced through the **network** command.
confed	Path was received from a confederation peer.
best	Path is selected as best.
multipath	Path is one of multiple paths selected for load-sharing purposes.
dampinfo	Indicates dampening information: Penalty—Current penalty for this path. Flapped—Number of times the route has flapped. In—Time (hours:minutes:seconds) since the network first flapped. Reuse in—Time (hours:minutes:seconds) after which the path is available. This field is displayed only if the path is currently suppressed.

Field	Description
Attributes after inbound policy was applied	Displays attributes associated with the received route, after any inbound policy has been applied. AGG—Aggregator attribute is present. AS—AS path attribute is present. ATOM—Atomic aggregate attribute is present. COMM—Communities attribute is present. EXTCOMM—Extended communities attribute is present. LOCAL—Local preference attribute is present. MET—Multi Exit Discriminator (MED) attribute is present. next hop—IP address of the next system used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network. ORG—Origin attribute is present.
origin	Origin of the path: IGP—Path originated from an Interior Gateway Protocol (IGP) and was sourced by BGP using a **network** or **aggregate-address** command. EGP—Path originated from an Exterior Gateway Protocol. incomplete—Origin of the path is not clear; in example, a route that is redistributed into BGP from an IGP.
neighbor as	First autonomous system (AS) number in the AS path.
aggregator	Indicates that the path was received with the aggregator attribute. The AS number and router-id of the system that performed the aggregation are shown.
metric	Value of the interautonomous system metric, otherwise known as the MED metric.
localpref	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system
aspath	AS path associated with the route.
community	Community attributes associated with the path. Community values are displayed in AA:NN format, except for the following well-known communities: Local-AS—Community with value 4294967043 or hex 0xFFFFFF03. Routes with this community value are not advertised outside the local autonomous system or confederation boundary. no-advertise—Community with value 4294967042 or hex 0xFFFFFF02. Routes with this community value are not advertised to any BGP peers. no-export—Community with value 4294967041 or hex 0xFFFFFF01. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation as the local router.

Field	Description
Extended community	Extended community attributes associated with the path. For known extended community types, the following codes may be displayed: RT—Route target community SoO—Site of Origin community LB—Link Bandwidth community
Originator	Router ID of the originating router when route reflection is used.
Cluster lists	Router ID or cluster ID of all route reflectors through which the route has passed.
Attributes after outbound policy was applied	Displays attributes associated with the received route, after any outbound policy has been applied. AGG—Aggregator attribute is present. AS—AS path attribute is present. ATOM—Atomic aggregate attribute is present. COMM—Communities attribute is present. EXTCOMM—Extended communities attribute is present. LOCAL—Local preference attribute is present. MET—Multi Exit Discriminator (MED) attribute is present. next hop—IP address of the next system used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network. ORG—Origin attribute is present.

show bgp route-policy

To display Border Gateway Protocol (BGP) information about networks that match an outbound route policy, use the **show bgp route-policy** command in config mode.

show bgp [**ipv4** { **unicast** | **multicast** | **labeled-unicast** | **all** | **tunnel** } | **all** { **unicast** | **multicast** | **all** | **labeled-unicast** | **tunnel** } | **vpnv4 unicast** [**rd** *rd-address*] | **vrf** { *vrf-name* | **all** } [**ipv4** { **unicast** | **labeled-unicast** }] **route-policy** *route-policy-name*

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
labeled-unicast	(Optional) Specifies labeled unicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
tunnel	(Optional) Specifies tunnel address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd *rd-address*	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 { **unicast** | **labeled-unicast** }	(Optional) For VRF, specifies IPv4 unicast or labeled-unicast address families.
route-policy-name	Name of a route policy.

Command Default

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

Config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session.

BGP contains a separate routing table for each address family and subaddress family combination that has been configured. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined.

A route policy must be configured to use this command. When the **show bgp route-policy** command is entered, routes in the specified BGP table are compared with the specified route policy, and all routes passed by the route policy are displayed.

If a pass clause is encountered while the route policy is being applied to the route and the route policy processing completes without hitting a drop clause, the route is displayed. The route is not displayed if a drop clause is encountered, if the route policy processing completes without hitting a pass clause, or if the specified route policy does not exist.

The information displayed does not reflect modifications the policy might make to the route. To display such modifications, use the **show bgp policy** command.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp route-policy** command :

```
RP/0/RP0:hostname# show bgp route-policy p1

BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 729
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
*  10.13.0.0/16       192.168.40.24                          0 1878 704 701 200 ?
*  10.16.0.0/16       192.168.40.24                          0 1878 704 701 i
```

This table describes the significant fields shown in the display.

Table 84: show bgp route-policy Field Descriptions

Field	Description
BGP router identifier	BGP identifier for the local system.

Field	Description
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** or **aggregate-address** command. e—Path originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit discriminator (MED) metric.

Field	Description
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

show bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the **show bgp summary** command in config mode.

show bgp [{**ipv4**{**unicast** | **multicast** | **labeled-unicast** | **all** | **tunnel** } | **all** {**unicast** | **multicast** | **all** | **labeled-unicast** | **tunnel** } | **vpnv4 unicast** | **vrf** {*vrf-name* | **all**}[{**ipv4** {**unicast** | **labeled-unicast** }}]}] **summary**

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
labeled-unicast	(Optional) Specifies labeled unicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
tunnel	(Optional) Specifies tunnel address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 { **unicast** | **labeled-unicast** }	(Optional) For VRF, specifies IPv4 unicast or labeled-unicast address families.

Command Default

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

Config

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session.

Use the **show bgp summary** command to display a summary of the neighbors for which the specified address family and subaddress family are enabled. If the neighbor does not have the specified address family and subaddress family enabled, it is not included in the output of the **show** command. If the **all** keyword is specified for the address family or subaddress family, a summary for each combination of address family and subaddress family is displayed in turn.

The table versions shown in the output (RcvTblVer, bRIB/RIB, SendTblVer, and TblVer) are specific to the specified address family and subaddress family. All other information is global.

The table versions provide an indication of whether BGP is up to date with all work for the specified address family and subaddress family.

- bRIB/RIB < RecvTblVer—Some received routes have not yet been considered for installation in the global routing table.
- TblVer < SendTblVer—Some received routes have been installed in the global routing table but have not yet been considered for advertisement to this neighbor.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp summary** command:

```
RP/0/RP0:hostname#show bgp summary

BGP router identifier 10.0.0.0, local AS number 2
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 1
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.

Process         RecvTblVer    bRIB/RIB  LabelVer  ImportVer  SendTblVer
Speaker                  1           0         1          1           0

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  St/PfxRcd
10.0.101.0        0     2       0       0        0    0    0 00:00:00 Idle
10.0.101.1        0     2       0       0        0    0    0 00:00:00 Idle
```

This table describes the significant fields shown in the display.

Table 85: show bgp summary Field Descriptions

Field	Description
BGP router identifier	IP address of the router.

Field	Description
local AS number	Autonomous system number set by the router bgp, on page 789 command. • Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. • Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. • Range for 4-byte Autonomous system numbers (ASNs) is asdot format is 1.0 to 65535.65535.
BGP generic scan interval	Interval (in seconds) between scans of the BGP table by a generic scanner.
BGP table state	State of the BGP database.
Table ID	BGP database identifier.
BGP main routing table version	Last version of the BGP database that was injected into the main routing table.
Dampening enabled	Displayed if dampening has been enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
BGP is operating in	Specifies BGP is operating in standalone mode.
Process	BGP process.
RecvTblVer	Last version used in the BGP database for received routes.
bRIB/RIB	Last version of the local BGP database that was injected into the main routing table.
LabelVer	Label version used in the BGP database for label allocation.
ImportVer	Last version of the local BGP database for importing routes.
SendTblVer	Latest version of the local BGP database that is ready to be advertised to neighbors.
Some configured eBGP neighbors do not have any policy	Some external neighbors exist that do not have both an inbound and outbound policy configured for every address family, using the **route-policy (BGP)** command. In this case, no prefixes are accepted and advertised to those neighbors.
Neighbor	IP address of a neighbor.
Spr	Speaker process that is responsible for the neighbor. Always 0.
AS	Autonomous system.
MsgRcvd	Number of BGP messages received from a neighbor.
MsgSent	Number of BGP messages sent to a neighbor.

Field	Description
TblVer	Last version of the BGP database that was sent to a neighbor.
InQ	Number of messages from a neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to a neighbor.
Up/Down	Length of time in (hh:mm:ss) that the BGP session has been in Established state, or the time since the session left Established state, if it is not established.
St/PfxRcd	If the BGP session is not established, the current state of the session. If the session is established, the number of prefixes the router has received from the neighbor. If the number of prefixes received exceeds the maximum allowed (as set by the **maximum-prefix** command), "(PfxRcd)" appears. If the connection has been shut down using the **shutdown** command, "(Admin)" appears. If the neighbor is external and it does not have an inbound and outbound policy configured for every address family, an exclamation mark (!) is inserted at the end of the state when using the **route-policy** (**BGP**) command. If the connection has been shut down due to out of memory (OOM), "(OOM)" appears.

table-policy

To apply a routing policy to routes being installed into the routing table, use the **table-policy** command in an appropriate configuration mode. To disable applying a routing policy when installing routes into the routing table, use the **no** form of this command.

table-policy *policy-name*
no table-policy [*policy-name*]

Syntax Description

policy-name	Name of the routing policy to apply.

Command Default

No policy is applied when routes are installed into the routing table.

Command Modes

IPv4 address family configuration

VRF IPv4 address family configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note Table policy provides users with the ability to drop routes from the RIB based on match criteria. This feature can be useful in certain applications and should be used with caution as it can easily create an unwanted traffic drop where BGP advertises routes to neighbors that BGP does not install in its global routing table and forwarding table.

Use the **table-policy** command to modify route attributes as the routes are installed into the routing table by Border Gateway Protocol (BGP). Commonly, it is used to set the traffic index attribute.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to apply the set-traffic-index policy to IPv4 unicast routes being installed into the routing table:

```
RP/0/RP0:hostname(config)# router bgp 1
RP/0/RP0:hostname(config-bgp)# address-family ipv4 unicast
RP/0/RP0:hostname(config-bgp-af)# table-policy set-traffic-index
```

update-source

To allow internal Border Gateway Protocol (iBGP) sessions to use the primary IP address from a particular interface as the local address when forming an iBGP session with a neighbor, use the **update-source** command in an appropriate configuration mode. To set the chosen local IP address to the nearest interface to the neighbor, use the **no** form of this command.

update-source *type interface-path-id*
no update-source [*type interface-path-id*]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

Best local address

Command Modes

Neighbor configuration

VRF neighbor configuration

Neighbor group configuration

Session group configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **update-source** command is commonly used with the loopback interface feature for iBGP sessions. The loopback interface is defined, and the interface address is used as the endpoint for a BGP session through the **update-source** command. This mechanism allows a BGP session to remain up even if the outbound interface goes down, provided there is another route to the neighbor.

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure this router to use the IP address from the Loopback0 interface when trying to open a session with neighbor 172.20.16.6:

```
RP/0/RP0:hostname(config)# router bgp 110
RP/0/RP0:hostname(config-bgp)# neighbor 172.20.16.6
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 110
RP/0/RP0:hostname(config-bgp-nbr)# update-source Loopback0
```

next-hop-self

To disable next-hop calculation and insert your own address in the next-hop field of Border Gateway Protocol (BGP) updates, use the next-hop-self command in an appropriate configuration mode. To enable **next-hop** calculation, use the **no** form of this command.

next-hop-self [*{inheritance-disable}*]
no next-hop-self [*{inheritance-disable}*]

Syntax Description

inheritance-disable	(Optional) Allows a next-hop calculation override when this feature may be inherited from a neighbor group or address family group.

Command Default

When this command is not specified, the software calculates the next hop for BGP updates accepted by the router.

Command Modes

IPv4 address family group configuration

IPv6 address family group configuration

VPNv4 address family group configuration

IPv4 neighbor address family configuration

VPNv4 neighbor address family configuration

IPv4 neighbor group address family configuration

IPv6 neighbor group address family configuration

VPNv4 neighbor group address family configuration

IPv4 labeled-unicast address family configuration

IPv6 labeled-unicast address family configuration

VRF labeled-unicast address family configuration

Command History

Release	Modification
Release 6.5.33	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **next-hop-self** command to set the BGP next-hop attribute of routes being advertised over a peering session to the local source address of the session.

This command is useful in nonmeshed networks in which BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

If this command is configured for a neighbor group or address family group, a neighbor using the group inherits the configuration. Configuring the command specifically for a neighbor overrides any inherited value.

Configuring the **next-hop-self** command under IPv4 labeled-unicast, IPv6 labeled-unicast, or VRF labeled-unicast address family configuration mode enables next-hop-self for labeled prefixes advertised to an iBGP peer.

Task ID

Task ID	Operation
bgp	read, write

The following example shows how to set the next hop of the update field for all IP Version 4 (IPv4) unicast routes advertised to neighbor 192.0.2.2 to an address of the local router:

```
RP/0/RP0:hostname(config)#router bgp 1
RP/0/RP0:hostname(config-bgp)#neighbor 192.0.2.2
RP/0/RP0:hostname(config-bgp-nbr)#remote-as 1
RP/0/RP0:hostname(config-bgp)#bfd multipier 3
RP/0/RP0:hostname(config-bgp)#bfd minimum-interval 2
RP/0/RP0:hostname(config-bgp-nbr)#bfdfast-detect
RP/0/RP0:hostname(config-bgp-nbr)#update-source hundredgige0/4/0/5.1
RP/0/RP0:hostname(config-bgp-nbr)#address-family ipv4 labeled unicast
RP/0/RP0:hostname(config-bgp-nbr)#route-reflector-client
RP/0/RP0:hostname(config-bgp-nbr)#next-hop-self
```

MPLS Traffic Engineering Commands

This chapter provides details of the commands used for configuring MPLS Traffic Engineering.

adjustment-threshold (MPLS-TE)

To configure the tunnel bandwidth change threshold to trigger an adjustment, use the **adjustment-threshold** command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the **no** form of this command.

adjustment-threshold *percentage* [**min** *minimum bandwidth*]
no adjustment-threshold *percentage* [**min** *minimum bandwidth*]

Syntax Description

percentage	Bandwidth change percent threshold to trigger an adjustment if the largest sample percentage is higher or lower than the current tunnel bandwidth. The range is from 1 to 100. The default is 5.
min *minimum bandwidth*	(Optional) Configures the bandwidth change value to trigger an adjustment. The tunnel bandwidth is changed only if the largest sample is higher or lower than the current tunnel bandwidth, in kbps. The range is from 10 to 4294967295. The default is 10.

Command Default

percentage: 5

minimum bandwidth: 10

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If you configure or modify the adjustment threshold while the automatic bandwidth is already running, the next band-aids application is impacted for that tunnel. The new adjustment threshold determines if an actual bandwidth takes place.

Examples

The following example configures the tunnel bandwidth change threshold to trigger an adjustment:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# auto-bw
RP/0/RP0:hostname(config-if-tunte-autobw)# adjustment-threshold 20 min 500
```

application (MPLS-TE)

To configure the application frequency, in minutes, for the applicable tunnel, use the **application** command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the **no** form of this command.

application *minutes*
no application *minutes*

Syntax Description

minutes	Frequency, in minutes, for the automatic bandwidth application. The range is from 5 to 10080 (7 days). The default is 1440.

Command Default

minutes : 1440 (24 hours)

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If you configure and modify the application frequency, the application period can reset and restart for that tunnel. The next bandwidth application for the tunnel happens within the specified minutes.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure application frequency to 1000 minutes for MPLS-TE interface 1:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# auto-bw
RP/0/RP0:hostname(config-if-tunte-autobw)# application 1000
```

bw-limit (MPLS-TE)

To configure the minimum and maximum automatic bandwidth to be set on a tunnel, use the **bw-limit** command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the **no** form of this command.

bw-limit min *bandwidth* {**max** *bandwidth*}
no bw-limit

Syntax Description

min *bandwidth*	Configures the minimum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 0.
max *bandwidth*	Configures the maximum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 4294967295.

Command Default

min: 0

max: 4294967295

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Both the **min** and **max** keywords must be configured.

The **bw-limit** command automatically sets the minimum bandwidth to the default value of 0, or the **bw-limit** command automatically sets the maximum to the default value of 4294967295 kbps.

If the value of the **min** keyword is greater than the **max** keyword, the **bw-limit** command is rejected. If you configure and modify the minimum or maximum bandwidth while the automatic bandwidth is already running, the next bandwidth application for that tunnel is impacted. For example, if the current tunnel requested bandwidth is 30 Mbps and the minimum bandwidth is modified to 50 Mbps, the next application sets the tunnel bandwidth to 50 Mbps.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure the minimum and maximum bandwidth for the tunnel:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# auto-bw
```

```
RP/0/RP0:hostname(config-if-tunte-autobw)# bw-limit min 30 max 80
```

clear mpls traffic-eng auto-bw (MPLS-TE EXEC)

To clear automatic bandwidth sampled output rates and to restart the application period for the specified tunnel, use the **clear mpls traffic-eng auto-bw** command in the EXEC mode.

clear mpls traffic-eng auto-bw{**all** | **internal** | **tunnel-te** *tunnel-number*}

Syntax Description

all	Clears the automatic bandwidth sampled output rates for all tunnels.
internal	Clears all the automatic bandwidth internal data structures.
tunnel-te *tunnel-number*	Clears the automatic bandwidth sampled output rates for a specific tunnel. The *tunnel-number* argument is the tunnel ID used to clear the sampled output rates.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If no tunnel is specified, the **clear mpls traffic-eng auto-bw** command clears all the automatic bandwidth enabled tunnels.

For each tunnel in which the automatic bandwidth adjustment is enabled, information is maintained about the sampled output rates and the time remaining until the next bandwidth adjustment. The application period is restarted and values such as the largest collected bandwidth get reset. The tunnel continues to use the current bandwidth until the next application.

Task ID

Task ID	Operations
mpls-te	execute

Examples

The following example displays the information for the automatic bandwidth for tunnel number 0 from the **show mpls traffic-eng tunnels auto-bw brief** command:

```
RP/0/RP0:hostname# show mpls traffic-eng tunnels 0 auto-bw brief

  Tunnel    LSP  Last appl  Requested  Signalled    Highest    Application
            Name     ID   BW(kbps)   BW(kbps)   BW(kbps)   BW(kbps)      Time Left
  ------------- ------ ---------- ---------- ---------- ---------- --------------
    tunnel-te0     278      100         100        100          150      12m 38s
```

The following example shows how to clear the automatic bandwidth sampled output rates for tunnel number 0:

```
RP/0/RP0:hostname# clear mpls traffic-eng auto-bw tunnel-te 0

RP/0/RP0:hostname# show mpls traffic-eng tunnels 0 auto-bw brief

  Tunnel    LSP  Last appl  Requested  Signalled    Highest    Application
            Name     ID   BW(kbps)   BW(kbps)   BW(kbps)   BW(kbps)       Time Left
  ------------- ------ ---------- ---------- ---------- ---------- --------------
    tunnel-te0     278      100         100        100          0         24m 0s
```

clear mpls traffic-eng fast-reroute log

To clear the log of MPLS fast reroute (FRR) events, use the **clear mpls traffic-eng fast-reroute log** command in the EXEC mode.

clear mpls traffic-eng fast-reroute log

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows sample output before clearing the log of FRR events:

```
RP/0/RP0:hostname# show mpls traffic-eng fast-reroute log

  Node     Protected LSPs  Rewrites When                   Switching Time
           Interface                                          (usec)
  -------- --------- ----- -------- ---------------------- --------------
  0/0/CPU0 PO0/1/0/1 1     1        Feb 27 19:12:29.064000      147
  0/1/CPU0 PO0/1/0/1 1     1        Feb 27 19:12:29.060093      165
  0/2/CPU0 PO0/1/0/1 1     1        Feb 27 19:12:29.063814      129
  0/3/CPU0 PO0/1/0/1 1     1        Feb 27 19:12:29.062861      128

RP/0/RP0:hostname# clear mpls traffic-eng fast-reroute log
```

destination (MPLS-TE)

To configure the destination address of a TE tunnel, use the **destination** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

destination *ip-address*
no destination *ip-address*

Syntax Description

ip-address	Destination address of the MPLS-TE router ID.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Note The tunnel destination address must be a unique MPLS-TE router ID; it cannot be an MPLS-TE link address on a node.

Use the **interface tunnel-mte** command to configure destinations for the Point-to-Multipoint (P2MP) TE tunnel and to enter P2MP destination interface configuration mode. The maximum number of destinations, which are configured under P2MP tunnels, is 500.

For P2MP tunnels, the **destination** command acts as a configuration mode. The **path-option** command is under the destination for P2MP; whereas, it is under the tunnel-te interface configuration mode for P2P tunnels.

For Point-to-Point (P2P) tunnels, the **destination** command is used as a single-line command.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the destination address for tunnel-te1 to 10.10.10.10:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-if)# destination 10.10.10.10
```

The following example shows how to set the destination address for tunnel-mte 10 to 150.150.150.150:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-mte10
RP/0/RP0:hostname(config-if)# destination 150.150.150.150
RP/0/RP0:hostname(config-if-p2mp-dest)#
```

fast-reroute

To enable fast-reroute (FRR) protection for an MPLS-TE tunnel, use the **fast-reroute** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

fast-reroute
no fast-reroute

Syntax Description

This command has no arguments or keywords.

Command Default

FRR is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

When a protected link used by the fast-reroutable label switched path (LSP) fails, the traffic is rerouted to a previously assigned backup tunnel. Configuring FRR on the tunnel informs all the nodes that the LSP is traversing that this LSP desires link/node/bandwidth protection.

You must allow sufficient time after an RSP RP switchover before triggering FRR on standby RSPs RPs to synchronize with the active RSP RP (verified using the **show redundancy** command). All TE tunnels must be in the recovered state and the database must be in the ready state for all ingress and egress line cards. To verify this information, use the **show mpls traffic-eng tunnels** and **show mpls traffic-eng fast-reroute database** commands.

Note Wait approximately 60 seconds before triggering FRR after verifying the database state.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enable FRR on an MPLS-TE tunnel:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# fast-reroute
```

mpls traffic-eng auto-bw apply (MPLS-TE)

To apply the highest bandwidth collected on a tunnel without waiting for the current application period to end, use the **mpls traffic-eng auto-bw apply** command in EXEC mode.

mpls traffic-eng auto-bw apply {**all** | **tunnel-te** *tunnel-number*}

Syntax Description

all	Applies the highest bandwidth collected instantly on all the automatic bandwidth-enabled tunnels.
tunnel-te *tunnel-number*	Applies the highest bandwidth instantly to the specified tunnel. The range is from 0 to 65535.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

The **mpls traffic-eng auto-bw apply** command can forcefully expire the current application period on a specified tunnel and immediately apply the highest bandwidth recorded so far instead of waiting for the application period to end on its own.

Note The predefined threshold check still applies on the configuration, and if the delta is not significant enough, the automatic bandwidth functionality overrides this command.

The bandwidth application is performed only if at least one output rate sample has been collected for the current application period.

To guarantee the application of a specific signaled bandwidth value when triggering a manual bandwidth application, follow these steps:

1. Configure the minimum and maximum automatic bandwidth to the bandwidth value that you want to apply by using the command.
2. Trigger a manual bandwidth application by using the **mpls traffic-eng auto-bw apply** command.
3. Revert the minimum and maximum automatic bandwidth value back to their original value.

Task ID

Task ID	Operations
mpls-te	execute

Examples

The following example applies the highest bandwidth to a specified tunnel:

```
RP/0/RP0:hostname# mpls traffic-eng auto-bw apply tunnel-te 1
```

mpls traffic-eng

To enter MPLS-TE configuration mode, use the **mpls traffic-eng** command in global configurtion mode.

mpls traffic-eng

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global Configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enter MPLS-TE configuration mode:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)#
```

r-mpls-te-path-protection-switchover

Syntax Description

Command Default

Command Modes

Command History

Release	Modification

Usage Guidelines

Task ID

Task ID	Operation

Example

r-mpls-te-reroute

Syntax Description

Command Default

Command Modes

Command History

Release	Modification

Usage Guidelines

Task ID

Task ID	Operation

Example

overflow threshold (MPLS-TE)

To configure the tunnel overflow detection, use the **overflow threshold** command in MPLS-TE automatic bandwidth interface configuration mode. To disable the overflow detection feature, use the **no** form of this command.

overflow threshold *percentage* [**min** *bandwidth*] **limit** *limit*
no overflow threshold

Syntax Description

percentage	Bandwidth change percent to trigger an overflow. The range is from 1 to 100.
min *bandwidth*	(Optional) Configures the bandwidth change value, in kbps, to trigger an overflow. The range is from 10 to 4294967295. The default is 10.
limit *limit*	Configures the number of consecutive collection intervals that exceeds the threshold. The bandwidth overflow triggers an early tunnel bandwidth update. The range is from 1 to 10. The default is none.

Command Default

The default value is disabled.

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If you modify the **limit** keyword, the consecutive overflows counter for the tunnel is also reset.

If you enable or modify the minimum value, the current consecutive overflows counter for the tunnel is also reset, which effectively restarts the overflow detection from scratch.

Several number of consecutive bandwidth samples are greater than the overflow threshold (bandwidth percentage) and the minimum bandwidth configured, then a bandwidth application is updated immediately instead of waiting for the end of the application period.

Overflow detection applies only to bandwidth increase. For example, an overflow can not be triggered even if bandwidth decreases by more than the configured overflow threshold.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure the tunnel overflow detection for tunnel-te 1:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te 1
```

```
RP/0/RP0:hostname(config-if)# auto-bw
RP/0/RP0:hostname(config-if-tunte-autobw)# overflow threshold 50 limit 3
```

path-option (MPLS-TE)

To configure a path option for an MPLS-TE tunnel, use the **path-option** command in tunnel-te interface configuration mode. To return to the default behavior, use the **no** form of this command.

path-option *preference-priority* [**protecting** *number*] { **dynamic** [**pce** [**address ipv4** *address*]] | **explicit** { **name** *path-name* | **identifier** *path-number* } [**protected-by** *path-option-level*] } **[attribute-set** *name]* [**isis** *instance-name* **level** *level*] [**lockdown**] [**sticky**] [**ospf** *instance-name* **area** { *value address* }] [**verbatim**]
no path-option *preference-priority* {**dynamic** [**pce** [**address ipv4** *address*]] | **explicit** {**name** *path-name* | **identifier** *path-number*}[**protected-by** *path-option-level*]} [**isis** *instance-name* **level** *level*] [**lockdown**] [**ospf** *instance-name* **area** {*value address*}] [**verbatim**]

Syntax Description

preference-priority	Path option number. Range is from 1 to 1000.
protecting *number*	Specifies a path setup option to protect a path. The range is from 1 to 1000.
dynamic	Specifies that label switched paths (LSP) are dynamically calculated.
pce	(Optional) Specifies that the LSP is computed by a Path Computation Element (PCE).
address	(Optional) Configures the address for the PCE.
ipv4 *address*	Configures the IPv4 address for the PCE.
explicit	Specifies that LSP paths are IP explicit paths.
name *path-name*	Specifies the path name of the IP explicit path.
identifier *path-number*	Specifies a path number of the IP explicit path.
protected-by *path-option-level*	(Optional) Configures path protection for an explicit path that is protected by another explicit path.
isis *instance-name*	(Optional) Limits CSPF to a single IS-IS instance and area.
attribute-set *name*	(Optional) Specifies the attribute set for the LSP.
level *level*	Configures the level for IS-IS. The range is from 1 to 2.
lockdown	(Optional) Specifies that the LSP cannot be reoptimized.
sticky	(Optional) Extended version of lockdown. LSP stays on the same path after change in resources. **Note** The sticky option can be configured only on the primary path option.
ospf *instance-name*	(Optional) Limits CSPF to a single OSPF instance and area.
area	Configures the area for OSPF.

value	Decimal value for the OSPF area ID.
address	IP address for the OSPF area ID.
verbatim	(Optional) Bypasses the Topology/CSPF check for explicit paths.

Command Default

No default behavior or values

Command Modes

Tunnel-te interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

You can configure several path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. The path setup preference is for lower (not higher) numbers, so option 1 is preferred.

When the lower number path option fails, the next path option is used to set up a tunnel automatically (unless using the lockdown option).

The **protecting** keyword specifies that you can configure path-protection for the primary LSP. The **protecting** keyword is available only for tunnel-gte interfaces.

You specify the backup path for the **path-option** command in case of the primary path failure.

CSPF areas are configured on a per-path-option basis.

The **dynamic** keyword is required to configure path-protection.

Any primary explicit path on a path protection enabled tunnel can be configured to be protected by an explicit path option level using **protected-by** keyword. Only one explicit protecting path is supported per path option.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure the tunnel to use a named IPv4 explicit path as verbatim and lockdown options for the tunnel. This tunnel cannot reoptimize when the FRR event goes away, unless you manually reoptimize it:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 explicit name test verbatim lockdown
```

The following example shows how to enable path protection on a tunnel to configure an explicit path:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 explicit name po4
```

```
RP/0/RP0:hostname(config-if)# path-option protecting 1 explicit name po6
```

The following example shows how to limit CSPF to a single OSPF instance and area:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 explicit name router1 ospf 3 area 7 verbatim
```

The following example shows how to limit CSPF to a single IS-IS instance and area:

```
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1 dynamic isis mtbf level 1 lockdown
```

path-selection cost-limit

To set the upper limit on the path aggregate admin-weight when computing paths for MPLS-TE LSPs, use the **path-selection cost-limit**command in an appropriate configuration mode. To remove the upper limit, use the no form of this command.

path-selection cost-limit *cost-limit*

no path-selection cost-limit *cost-limit*

Syntax Description

cost-limit	Configures the path-selection cost-limit value. The range is from 1 to 4294967295.

Command Default

None

Command Modes

Global configuration

Interface tunnel TE configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Path-selection cost-limit configuration works on MPLS TE tunnels and enables the creation of LSPs, only if the path aggregate admin-weight is less than the specified path cost limit.

Example

This example shows how to use the **path- selection cost-limit** command:

```
RP/0/RP0:hostname:router #  mpls traffic-eng path-selection cost-limit 16777199
```

show mpls traffic-eng tunnels

To display information about MPLS-TE tunnels, use the **show mpls traffic-eng tunnels** command in the EXEC mode.

show mpls traffic-eng tunnels [*tunnel-id*] [**detail** | **tabular**]

Syntax Description

tunnel-id	Tunnel identification number. Range is from 0 to 65535.
detail	Displays detailed information for the specified tunnel-id.
tabular	Displays tunnel information in table-format.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read

Example

This example shows how to use the **show mpls traffic-eng tunnels** command with the **detail** keyword:

```
show mpls traffic-eng tunnels 1000 detail
Name: tunnel-te1000  Destination: 104.0.0.1  Ifhandle:0x8001afc
  Signalled-Name: NCS4K-R11_t1000
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 1,  type explicit path01 (Basis for Setup, path weight 30)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 10 kbps  CT0
    Creation Time: Sat Jan  7 16:33:48 2017 (00:01:21 ago)
  Config Parameters:
    Bandwidth:       10 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (interface)
    Path Selection:
      Tiebreaker: Min-fill (default)
    Hop-limit: disabled
    Cost-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
```

```
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (default)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Enabled, Protection Desired: Any
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    Soft Preemption: Disabled
  SNMP Index: 133
  Binding SID: None
  History:
    Tunnel has been up for: 00:01:06 (since Sat Jan 07 16:34:03 UTC 2017)
    Current LSP:
      Uptime: 00:01:06 (since Sat Jan 07 16:34:03 UTC 2017)
  Current LSP Info:
    Instance: 2, Signaling Area: IS-IS 100 level-2
    Uptime: 00:01:06 (since Sat Jan 07 16:34:03 UTC 2017)
    Outgoing Interface: TenGigE0/4/0/2, Outgoing Label: 24099
    Router-IDs: local      102.0.0.1
                downstream 107.0.0.1
    Soft Preemption: None
    SRLGs: not collected
    Path Info:
      Outgoing:
        Explicit Route:
          Strict, 3.27.1.2
          Strict, 3.67.1.2
          Strict, 3.67.1.1
          Strict, 3.46.1.2
          Strict, 3.46.1.1
          Strict, 104.0.0.1

      Record Route: Disabled
      Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
      Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set
                          Soft Preemption Desired: Not Set
    Resv Info:
      Record Route:
        IPv4 107.0.0.1, flags 0x20 (Node-ID)
        Label 24099, flags 0x1
        IPv4 3.27.1.2, flags 0x0
        Label 24099, flags 0x1
        IPv4 106.0.0.1, flags 0x20 (Node-ID)
        Label 24099, flags 0x1
        IPv4 3.67.1.1, flags 0x0
        Label 24099, flags 0x1
        IPv4 104.0.0.1, flags 0x20 (Node-ID)
        Label 3, flags 0x1
        IPv4 3.46.1.1, flags 0x0
        Label 3, flags 0x1
      Fspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
  Persistent Forwarding Statistics:
    Out Bytes: 0
    Out Packets: 0

LSP Tunnel 104.0.0.1 1000 [2] is signalled, Signaling State: up
  Tunnel Name: NCS4K-R10_t1000 Tunnel Role: Tail
  InLabel: TenGigE0/4/0/2, implicit-null
  Signalling Info:
    Src 104.0.0.1 Dst 102.0.0.1, Tun ID 1000, Tun Inst 2, Ext ID 104.0.0.1
    Router-IDs: upstream   107.0.0.1
```

```
            local      102.0.0.1
    Bandwidth: 10 kbps (CT0) Priority:  7  7 DSTE-class: 0
    Soft Preemption: None
    SRLGs: not collected
    Path Info:
      Incoming Address: 3.27.1.1
      Incoming:
      Explicit Route:
        Strict, 3.27.1.1
        Strict, 102.0.0.1

      Record Route: Disabled
      Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
      Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set
                          Soft Preemption Desired: Not Set
    Resv Info: None
      Record Route: Empty
      Fspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
Displayed 1 (of 100) heads, 0 (of 0) midpoints, 1 (of 100) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

show mpls traffic-eng tunnels auto-bw brief

To display the list of automatic bandwidth enabled tunnels, and to indicate if the current signaled bandwidth of the tunnel is identical to the bandwidth that is applied by the automatic bandwidth, use the **show mpls traffic-eng tunnels auto-bw brief** command in the EXEC mode.

show mpls traffic-eng tunnels auto-bw brief

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **show mpls traffic-eng tunnels auto-bw brief** command to determine if the automatic bandwidth application has been applied on a specified tunnel. If a single tunnel is specified, only the information for that tunnel is displayed.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following sample output shows the list of automatic bandwidth enabled tunnels:

```
RP/0/RP0:hostname# show mpls traffic-eng tunnels auto-bw brief

  Tunnel    LSP  Last appl  Requested  Signalled    Highest    Application
  Name       ID   BW(kbps)   BW(kbps)   BW(kbps)   BW(kbps)      Time Left
  ------------- ------ ---------- ---------- ---------- ---------- --------------
  tunnel-te0      1           10         10         50      2h 5m
  tunnel-te1      5          500        300        420     1h 10m
```

This table describes the significant fields shown in the display.

Table 86: show mpls traffic-eng tunnels auto-bw brief Field Descriptions

Field	Description
Tunnel Name	Name for the tunnel.
LSP ID	ID of the Label Switched Path that is used by the tunnel.
Last appl BW (kbps)	Last bandwidth applied (for example, requested) by the automatic-bandwidth feature for the tunnel.

Field	Description
Requested BW (kbps)	Bandwidth that is requested for the tunnel.
Signalled BW (kbps)	Bandwidth that is actually signalled for the tunnel.
Highest BW (kbps)	Highest bandwidth measured since the last start of the application interval.
Application Time Left	Time left until the application period ends for this tunnel.

show mpls traffic-eng fast-reroute database

To display the fast reroute database information, use the **show mpls traffic-eng fast-reroute database**command in the EXEC mode.

show mpls traffic-eng fast-reroute database

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.
Release 6.5.3.1	LAG interface was supported.

Usage Guidelines No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read

Example

This example shows how to use the **show mpls traffic-eng fast-reroute database** command:

```
show mpls traffic-eng fast-reroute database
Tunnel head FRR information:
Tunnel       Out Intf : Label   FRR Intf : Label   Status
------------ ------------------ ------------------ -------
tt1000       Hu0/3/0/0:24201    tt4000:24201       Ready
tt1002       Hu0/3/0/0:24103    tt4000:24103       Ready
tt1003       Hu0/3/0/0:24104    tt4000:24104       Ready
tt1001       Hu0/3/0/0:24102    tt4000:24102       Ready
tt1004       Hu0/3/0/0:24105    tt4000:24105       Ready
tt1005       Hu0/3/0/0:24106    tt4000:24106       Ready
tt1006       Hu0/3/0/0:24107    tt4000:24107       Ready
tt1007       Hu0/3/0/0:24108    tt4000:24108       Ready
tt1008       Hu0/3/0/0:24109    tt4000:24109       Ready
tt1009       Hu0/3/0/0:24110    tt4000:24110       Ready
tt1010       Hu0/3/0/0:24111    tt4000:24111       Ready
tt1011       Hu0/3/0/0:24112    tt4000:24112       Ready
tt1012       Hu0/3/0/0:24113    tt4000:24113       Ready
tt1013       Hu0/3/0/0:24114    tt4000:24114       Ready
tt1014       Hu0/3/0/0:24115    tt4000:24115       Ready
tt1015       Hu0/3/0/0:24116    tt4000:24116       Ready
tt1016       Hu0/3/0/0:24117    tt4000:24117       Ready
tt1017       Hu0/3/0/0:24118    tt4000:24118       Ready
```

```
tt1018       Hu0/3/0/0:24119    tt4000:24119       Ready
tt1019       Hu0/3/0/0:24120    tt4000:24120       Ready
tt1020       Hu0/3/0/0:24121    tt4000:24121       Ready
tt1021       Hu0/3/0/0:24122    tt4000:24122       Ready
tt1022       Hu0/3/0/0:24123    tt4000:24123       Ready
tt1023       Hu0/3/0/0:24124    tt4000:24124       Ready
tt1024       Hu0/3/0/0:24125    tt4000:24125       Ready
tt1025       Hu0/3/0/0:24126    tt4000:24126       Ready
tt1026       Hu0/3/0/0:24127    tt4000:24127       Ready
tt1027       Hu0/3/0/0:24128    tt4000:24128       Ready
tt1028       Hu0/3/0/0:24129    tt4000:24129       Ready
tt1029       Hu0/3/0/0:24130    tt4000:24130       Ready
tt1030       Hu0/3/0/0:24131    tt4000:24131       Ready
```

This example shows the sample output of **show mpls traffic-eng fast-reroute database** command with LAG interface:

```
show mpls traffic-eng fast-reroute database
Sun Jun  7 18:45:12.640 UTC
Tunnel head FRR information:
Tunnel       Out Intf : Label   FRR Intf : Label   Status
------------ ------------------ ------------------ -------
tt1          BE1:20010          tt3001:20010       Ready
tt2          BE1:20011          tt3001:20011       Ready
tt3          BE1:20012          tt3001:20012       Ready
tt4          BE1:20013          tt3001:20013       Ready
tt5          BE1:20014          tt3001:20014       Ready
tt6          BE1:20015          tt3001:20015       Ready
tt7          BE1:20016          tt3001:20016       Ready
tt8          BE1:20017          tt3001:20017       Ready
tt9          BE1:20018          tt3001:20018       Ready
tt10         BE1:20019          tt3001:20019       Ready
tt11         BE1:20020          tt3001:20020       Ready
tt12         BE1:20021          tt3001:20021       Ready
tt13         BE1:20022          tt3001:20022       Ready
tt14         BE1:20023          tt3001:20023       Ready
tt15         BE1:20024          tt3001:20024       Ready
tt16         BE1:20025          tt3001:20025       Ready
tt17         BE1:20026          tt3001:20026       Ready
tt18         BE1:20027          tt3001:20027       Ready
tt19         BE1:20028          tt3001:20028       Ready
tt20         BE1:20029          tt3001:20029       Ready
```

show mpls traffic-eng fast-reroute log

To display the log of MPLS FRR events, use the **show mpls traffic-eng fast-reroute log** command in the EXEC mode.

show mpls traffic-eng fast-reroute log

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 6.5.3.1	This command was introduced.

Usage Guidelines No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read

Example

This example shows how to use the **show mpls traffic-eng fast-reroute log** command:

```
show mpls traffic-eng fast-reroute log
Sun Jun  7 18:47:48.643 UTC

Location Protected              When                    Switching Time
         Interface                                          (usec)
-------- ---------------------- ----------------------- --------------
0/RP0    BE1                    Jun  7 18:47:43.371781        0
```

show mpls traffic-eng forwarding tunnels

To display the forwarding information of tunnels, use the **show mpls traffic-eng forwarding tunnels**command in EXEC mode.

show mpls traffic-eng forwarding tunnels [*tunnel-id*][**detail**]

Syntax Description

tunnel-id	Tunnel identification number. Displays forwarding information for the specified tunnel-id.
detail	Displays tunnel information in detail.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read

Example

This example show how to use the **show mpls traffic-eng forwarding tunnels** command with the **detail** keyword:

```
Tunnel        Outgoing    Outgoing     Next Hop        Bytes
Name          Label       Interface                    Switched
------------- ----------- ------------ --------------- ------------
tt1000            24201       Hu0/3/0/0    3.46.1.2        0
     Updated: Jan  7 16:35:00.454
     Version: 108324, Priority: 2
     Label Stack (Top -> Bottom): { 24201 }
     Local Label: 24184
     NHID: 0x0, Encap-ID: N/A, Path idx: 0, Backup path idx: 0, Weight: 0
     MAC/Encaps: 14/18, MTU: 1500
     Packets Switched: 0

  Interface Name: tunnel-te1000, Interface Handle: 0x0800002c, Local Label: 24184
  Forwarding Class: 0, Weight: 0
  Packets/Bytes Switched: 0/0
```

show pce ipv4

To display the status of the path computation element (PCE) peer, prefix, tunnel, or topology, use the **show pce ipv4** command in EXEC mode.

Note This command should be run for NCS 5500.

show pce ipv4 { **peer** | **topology** [**summary**] }

Syntax Description

peer	Displays the PCE peer database.
topology	Displays detailed PCE topology information.
summary	Displays a summary of the PCE topology information.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines No specific usage guidelines.

Task ID

Task ID	Operation

Example

This example shows how to display the PCE peer information:

```
RP/0/RP0/CPU0:NCS5500-10#show pce ipv4 peer
PCE's peer database:
--------------------
Peer address: 198.51.100.1
  State: Up
  Capabilities: Stateful, Update, Instantiation
RP/0/RP0/CPU0:NCS5500-10#show pce lsp tabular
PCC               Tunnel Name   Color   Source          Destination    TunID  LSPID  Admin
  Oper
198.51.100.1       PCEP-TEST       0     198.51.100.1     198.51.100.3   00     141    up
    up  □ Manual
198.51.100.1       m1              0     198.51.100.1     198.51.100.3   5000   8      up
    up  □ PCE Initiated (CURL)
```

This example shows how to display summary of the PCE topology information:

```
RP/0/RP0/CPU0:NCS5500-10#show pce ipv4 topology summary
PCE's topology database summary:
--------------------------------
Topology nodes:                4
Prefixes:                      4
Prefix SIDs:
  Total:                       0
  Regular:                     0
  Strict:                      0
Links:
  Total:                       8
  EPE:                         0
Adjacency SIDs:
  Total:                       0
  Unprotected:                 0
  Protected:                   0
  EPE:                         0
Private Information:
Lookup Nodes                   4
Consistent                   yes
Update Stats (from IGP and/or BGP):
  Nodes added:                 4
  Nodes deleted:               0
  Links added:                11
  Links deleted:               3
  Prefix added:               12
  Prefix deleted:              0
Topology Ready Summary:
  Ready:                     yes
  PCEP allowed:              yes
  Last HA case:          startup
  Timer value (sec):         300
  Timer:
    Running: no
```

show pce lps

To display the detailed information of an LSP present in the PCE's LSP database, in table format, use the **show pce lps** command in EXEC mode.

Note This command should be run for NCS 5500.

show pce lps { **tabular** }

Syntax Description

tabular	Displays lsp information in table-format.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines No specific usage guidelines.

Task ID

Task ID	Operation

Example

This example shows how to display the lsp information:

```
RP/0/RP0/CPU0:NCS5500-10#show pce lsp tabular
Tue Feb 9 11:14:08.858 UTC
PCC           TunnelName      Color  Source      Destination  TunID  LSPID  Admin Oper
198.51.100.1  NCS4016-1_t1000   0   198.51.100.1 198.51.100.2 1000   10     up    up
198.51.100.1  NCS4016-1_t300    0   198.51.100.1 198.51.100.2 300    6      up    up
198.51.100.1  m                 0   198.51.100.1 198.51.100.2 5000   3      up    up
198.51.100.1  mapm1             0   198.51.100.1 198.51.100.2 5003   3      up    up
198.51.100.1  te99              0   198.51.100.1 198.51.100.2 5002   4      up    up
198.51.100.1  tunnel-te500      0   198.51.100.1 198.51.100.2 5001   3      up    up
```

show mpls traffic-eng pce peer

To display the status of the path computation element (PCE) peer address and state, use the **show mpls traffic-eng pce peer** command in EXEC mode XR EXEC mode.

show mpls traffic-eng pce peer

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXECXR EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following sample output shows the status of both the PCE peer and state:

```
RP/0/RP0:NCS4016-1#show mpls tr pce peer
Address          Precedence    State         Learned From
---------------- ------------ ------------ --------------------
203.0.113.1        10           Up           Static config
RP/0/RP0:NCS4016-1#show mpls tr pce lsp-database brief
PCE ID Tun ID LSP ID Symbolic-name  Destination     State Type DLG
------ ------ ------ -------------------- --------------- ----- ---- ---
301    300    130    PCEP-TEST     198.51.100.3        Up    Conf yes *Manual + PCE Delegated
5001    5000   8      m1        198.51.100.3        Up    Init yes . .Curl or PCE Initiated
• CURL COMMAND INITIATED TUNNEL
*Manually CONFIGURED under HEADEND Node (Tunnel-te 300)\
```

show mpls traffic-eng pce lsp-database

To display information about all LSPs and their attributes, use the **show mpls traffic-eng pce lsp-database** command in EXEC mode XR EXEC mode.

show mpls traffic-eng pce lsp-database

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes EXECXR EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines No specific usage guidelines.

Task ID

Task ID	Operation
mpls-te	read

Example

The following shows a sample output for the **show mpls traffic-eng pce lsp-database** command:

```
RP/0/RP0:NCS4016-1#show mpls tr pce lsp-database symbolic-name PCEP-TEST detail
Thu Jul 30 16:50:05.121 IST
Symbolic name: PCEP-TEST
Session internal LSP ID: 301
Stateful Request Parameters ID: 0
Path Setup Type: 0 - (RSVP)
Request queue size: 0
Create: FALSE
    Created by: Not set
Delegatable: TRUE
    Delegation status: Delegated
    Delegated to: Speaker-entity-id: Not set ip: 203.0.113.1
Destination: 198.51.100.3    Source: 198.51.100.1
LSP Object:
    Administrative: Up
    Operational state: Up
    Identifiers:
        Sender Address: 198.51.100.1
        TE LSP ID: 141
        Tunnel ID: 300
        Extended tunnel ID: 0x3030303
    Binding SID: 24012
LSP Path Object:
    Explicit Route Object:
        Cost: 0
```

```
        1.  ipv4: 209.165.200.4/32 (strict)
        2.  ipv4: 51.0.0.2/32 (strict)
LSP Attributes:
        Exclude any: 0
        Include any: 0
        Include all: 0
        Setup priority: 7
        Hold priority: 7
        Local Protection Bit: TRUE
    Reported Route Object:
        Cost: 0
        1.  ipv4: 198.51.100.2/32
        2. label: 26004 (global)
        3.  ipv4: 209.165.200.4/32
        4. label: 26004 (global)
        5.  ipv4: 198.51.100.3/32
        6. label: 0 (global)
        7.  ipv4: 51.0.0.2/32
        8. label: 0 (global)
    Bandwidth:  0 Bps (0 kbps)
    Reoptimized bandwidth: Not set
    Applied bandwidth: Not set
    Metric:
        Cost: 20        Type: IGP
    Vendor Specific Information:
        Forward-Class: Not set
        Load Share: Not set
        Backup path: Not set
```

Bidirectional Forwarding Commands

This chapter provides details of the commands used for configuring Bidirectional Forwarding for Label Switched Paths.

clear bfd counters

To clear Bidirectional Forwarding Detection (BFD) counters, use the **clear bfd counters** command in the EXEC mode.

clear bfd counters {**ipv4** | [{**singlehop** | }] | [{**singlehop** | }] | **all** | **label**} [**packet**] [**timing**] [**interface** *type interface-path-id*] **location** *node-id*

Syntax Description

ipv4	(Optional) Clears BFD over IPv4 information only.
singlehop	(Optional) Clears BFD singlehop information only.
all	(Optional) Clears BFD over IPv4 information.
packet	(Optional) Specifies that packet counters are cleared.
timing	(Optional) Specifies that timing counters are cleared.
interface	(Optional) Specifies the interface from which the BFD packet counters are cleared.
type	Specifies the interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	Clears BFD counters from the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The default is the default address family identifier (AFI) that is set by the **set default-afi** command.

Command Modes

XR EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.

- *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
bgp	read, write
ospf	read, write
isis	read, write
mpls-te	read, write

Examples

The following example shows how to clear the BFD IPv4 timing counters:

```
RP/0/RP0:hostname# clear bfd counters ipv4 timing location 0/5/cpu0
```

bfd address-family

Use the **bfd address-family** command in interface configuration mode to perform the following.

- Specify the destination address for BFD sessions on bundle member links.
- Enable IPv4 BFD sessions on bundle member links.
- Specify the minimum interval for asynchronous mode control packets on IPv4 BFD sessions on bundle member links.
- Specify a number that is used as a multiplier with the minimum interval to determine BFD control packet failure detection times and transmission intervals for IPv4 BFD sessions on bundle member links.

bfd address-family ipv4 {destination *ip-address* | **fast-detect** | **minimum-interval** *milliseconds* | **multiplier** *multiplier* **}**

Syntax Description

destination *ip-address*	32-bit IPv4 address in dotted-decimal format (A.B.C.D).
fast-detect	Enables IPv4 BFD sessions on bundle member links.
minimum-interval *milliseconds*	Shortest interval between sending BFD control packets to a neighbor. The range is from 4 to 30000.
multiplier *multiplier*	Number from 2 to 50. It is recommended to have multiplier value of 3.

Command Default

None.

Command Modes

Neighbor configuration

Session group configuration

Neighbor group configuration

Interface configuration

Interface configuration

Router configuration

Area configuration

Area interface configuration

Interface configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
bgp	read, write
isis	read, write
mpls-te	read, write
ospf	read, write

Examples

The following example shows how to use the **bfd-address-family** command to set specific parameters:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 minimum-interval 2000
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 multiplier 3
```

bfd fast-detect

To enable Bidirectional Forwarding Detection (BFD) to detect failures in the path between adjacent forwarding engines, use the **bfd fast-detect** command in the appropriate configuration mode. To return the software to the default state in which BFD is not enabled, use the **no** form of this command.

bfd fast-detect
no bfd fast-detect

Syntax Description

No supported keywords or arguments

Command Default

BFD detection of failures in the path between adjacent forwarding engines is disabled.

Command Modes

Neighbor configuration

Session group configuration

Neighbor group configuration

Interface configuration

Interface configuration

Router configuration

Area configuration

Area interface configuration

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **bfd fast-detect** command to provide protocol- and media-independent, short-duration failure detection of the path between adjacent forwarding engines, including the interfaces and data links.

BFD must be configured on directly connected neighbors for a BFD session to be established between the neighbors.

BFD can support multihop for internal and external BGP peers.

In OSPF environments, the setting of the **bfd fast-detect** command is inherited from the highest-level configuration mode in which the command was configured. From the lowest to the highest configuration modes, the inheritance rules are as follows:

- If you enable BFD in area interface configuration mode, it is enabled on the specified interface only.
- If you enable BFD in area configuration mode, it is enabled on all interfaces in the specified area.
- If you enable BFD in router configuration mode, it is enabled on all areas and all associated interfaces in the specified routing process.

The **disable** keyword is available in the following modes: BGP configuration, OSPF area configuration, OSPF area interface configuration, OSPFv3 area configuration, and OSPFv3 area interface configuration . In OSPF environments, the **disable** option enables you to override the inheritance rules described previously. For example, if you enable BFD in an OSPF area, BFD is enabled on all interfaces in that area. If you do not want BFD running on one of the interfaces in that area, you must specify the **bfd fast-detect disable** command for that interface only.

Task ID

Task ID	Operations
bgp	read, write
isis	read, write
mpls-te	read, write
ospf	read, write

Examples

The following example shows how to configure BFD on a BGP router:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-te)# bfd fast-detect
```

bfd minimum-interval

To specify the minimum control packet interval for BFD sessions for the corresponding BFD configuration scope, use the **bfd minimum-interval** command in the appropriate configuration mode. To return the router to the default setting, use the **no** form of this command.

bfd minimum-interval *milliseconds*
no bfd minimum-interval [*milliseconds*]

Syntax Description

milliseconds	Interval between sending BFD hello packets to the neighbor. For Flex LSP, the range is 4 to 2000 milliseconds.

Command Default

BGP *interval*: 50 milliseconds

IS-IS *interval*: 150 milliseconds

OSPF and OSPFv3 *interval*: 150 milliseconds

MPLS-TE *interval*: 15 milliseconds

PIM *interval*: 150 milliseconds

Flex LSP *interval*: 100 milliseconds

Command Modes

Router configuration

Interface configuration

MPLS TE configuration

Router configuration

Area configuration

Area interface configuration

Router configuration

Area configuration

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

In OSPF and OSPFv3 environments, the setting of the **bfd minimum-interval** command is inherited from the highest-level configuration mode in which the command was configured. From the lowest to the highest configuration modes, the inheritance rules are as follows:

- If you configure the minimum interval in area interface configuration mode, the updated interval affects the BFD sessions on the specified interface only.
- If you configure the minimum interval in area configuration mode, the updated interval affects the BFD sessions on all interfaces in the specified area.

- If you configure the minimum interval in router configuration mode, the updated interval affects the BFD sessions in all areas and all associated interfaces in the specified routing process.

If desired, you can override these inheritance rules by explicitly configuring the **bfd minimum-interval** command for a specific area interface or area.

Note When multiple applications share the same BFD session, the application with the most aggressive timer wins locally. Then, the result is negotiated with the peer router.

Keep the following router-specific rules in mind when configuring the minimum BFD interval:

- The maximum rate in packets-per-second (pps) for BFD sessions is linecard-dependent. If you have multiple linecards supporting BFD, then the maximum rate for BFD sessions per system is the supported linecard rate multiplied by the number of linecards.
  - The maximum rate for BFD sessions per linecard is 7000 pps.
  - The maximum rate for BFD sessions per linecard is 9600 pps.
  - The maximum rate for BFD sessions per linecard is 1334 pps.
- If a session is running in asynchronous mode without echo, then PPS used for this session is (1000 / asynchronous interval in milliseconds).
- If a session is running in asynchronous mode with echo, then PPS used for this session is (1000 / echo interval in milliseconds).

  This is calculated as: 1000 / value of the **bfd minimum-interval** command.

Note The rate for BFD sessions on bundle member links is calculated differently. For more information, see the **bfd address-family ipv4 minimum-interval** command.

- The maximum number of all BFD sessions per linecard is 1024.
- The maximum number of all BFD sessions per linecard is 1440.
- When asynchronous mode is available, the minimum interval must be greater than or equal to 15 milliseconds for up to 100 sessions on the line card. If you are running the maximum of 1024 sessions, the failure detection interval must be greater than or equal to 150 milliseconds.
- When asynchronous mode is available, the minimum interval must be greater than or equal to 250 milliseconds, with a multiplier of 3 for up to 100 sessions per line card
- When asynchronous mode is available, the minimum interval must be greater than or equal to 15 milliseconds for up to 100 sessions on the line card. If you are running the maximum of 1440 sessions, the failure detection interval must be greater than or equal to 150 milliseconds.
- When echo mode is available, the minimum interval must be greater than or equal to 15 milliseconds for up to 100 sessions on the line card. If you are running the maximum of 1024 sessions, the failure detection interval must be less than or equal to 150 milliseconds.
- When echo mode is available, the minimum interval must be 50 milliseconds with a multiplier of 3.
- When echo mode is available, the minimum interval must be greater than or equal to 15 milliseconds for up to 100 sessions on the line card. If you are running the maximum of 1440 sessions, the failure detection interval must be less than or equal to 150 milliseconds.

Task ID

Task ID	Operations
bgp	read, write
isis	read, write
mpls-te	read, write
ospf	read, write

Examples

The following example shows how to set the BFD minimum interval for a BGP routing process:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-te)# bfd minimum-interval 200
```

The following example shows the configuration of an OSPFv3 routing process named san_jose. The example shows two areas, each of which includes tengige interfaces. In area 0, the minimum interval is set to 200 at the area level, which means that by virtue of the inheritance rules, the same value is set on all interfaces within the area except those on which a different value is explicitly configured. Given this rule, tengige interface 1/0/0/0 uses the interval of 200, which is inherited from the area, while interface 2/0/0/0 uses the explicitly configured value of 300.

In area 1, the minimum interval is not configured at the area or interface levels, which means that interfaces 3/0/0/0 and 4/0/0/0 use the default interval of 150.

```
router ospfv3 san_jose
bfd fast-detect
    area 0
bfd minimum-interval 200
int gige 1/0/0/0
        !
int gige 2/0/0/0
bfd minimum-interval 300
        !
    !
    area 1
int gige 3/0/0/0
        !
int gige 4/0/0/0
!
    !
```

bfd mode

Te enable IETF mode for BFD over bundle, use the **bfd mode** command in interface configuration mode.

bfd mode ietf

Syntax Description

ietf	Specifies the use of IETF mode for BFD over bundle.

Command Default

The default member mode is ietf.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

If the BFD modeis configured when the bundle is being created, the configuration goes through. This is because, both the BFD state as well as the bundle state are 'down' during bundle creation. To apply the mode change for existing sessions, bring down and then recreate the BFD sessions for that bundle. This command is supported on only the bundle interfaces.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to enable IETF mode for BFD over bundle for the specified bundle.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 fast-detect
RP/0/RP0:hostname(config-if)# bfd mode ietf
```

bfd multiplier

To set the Bidirectional Forwarding Detection (BFD) multiplier, use the **bfd multiplier** command in the appropriate configuration mode. To return the router to the default setting, use the **no** form of this command.

bfd multiplier *multiplier*
no bfd multiplier [*multiplier*]

Syntax Description

multiplier	Number of times a packet is missed before BFD declares the neighbor down. The ranges are as follows: • BGP—2 to 16 • IS-IS—2 to 50 • OSPF and OSPFv3—2 to 50 • PIM—2 to 50

Command Default

The default multiplier is 3.

Command Modes

Router configuration

Interface configuration

Router configuration

Area configuration

Area interface configuration

Interface configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

In OSPF environments, the setting of the **bfd multiplier** command is inherited from the highest-level configuration mode in which the command was configured. From the lowest to the highest configuration modes, the inheritance rules are as follows:

- If you configure a multiplier in area interface configuration mode, the updated multiplier affects the BFD sessions on the specified interface only.
- If you configure a multiplier in area configuration mode, the updated multiplier affects the BFD sessions on all interfaces in the specified area.
- If you configure a multiplier in router configuration mode, the updated multiplier affects the BFD sessions in all areas and all associated interfaces in the specified routing process.

If desired, you can override these inheritance rules by explicitly configuring the **bfd multiplier** command for a specific area interface or area.

If the multiplier is changed using the **bfd multiplier** command, the new value is used to update all existing BFD sessions for the protocol (BGP, IS-IS, MPLS-TE, OSPF, or OSPFv3) .

Task ID

Task ID	Operations
bgp	read, write
isis	read, write
mpls-te	read, write
ospf	read, write

Examples

The following example shows how to set the BFD multiplier in a BGP routing process:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-te)# bfd multiplier 2
```

bundle minimum-active

To set the minimum amount of bandwidth required before a user can bring up a specific bundle or to set the number of active links required to bring up a specific bundle, use the **bundle minimum-active** command in interface configuration mode.

bundle minimum-active {bandwidth *kbps* **| links** *links* **}**

Syntax Description

kbps	Sets the minimum amount of bandwidth required before a bundle can be brought up or remain up. The range is from 1 through a number that varies depending on the platform and the bundle type.
links	Sets the number of active links required before a bundle can be brought up or remain up. The range is from 1 to 16.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
bundle	read, write

Examples

The following example shows how to configure the minimum thresholds to maintain an active bundle.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 580000
RP/0/RP0:hostname(config-if)# bundle minimum-active links 2
```

show bfd

To display Bidirectional Forwarding Detection (BFD) information for a specific location, use the **show bfd** command in EXEC mode.

show bfd [{**ipv4** | [{**singlehop** | }] | **all**|**label**}]**interface**[{**destination** | }] [**location** *node-id*]

Syntax Description

ipv4	(Optional) Displays BFD over IPv4 information only.
multihop	(Optional) Displays BFD multihop information only.
singlehop	(Optional) Displays BFD singlehop information only.
all	(Optional) Displays BFD over IPv4 information.
label	(Optional) Displays the BFD label information.
interface	Specifies the BFD interface.
destination	(Optional) Specifies the destination IPv4 unicast address.
source	(Optional) Specifies the source IPv4 unicast address.
location *node-id*	Displays BFD information for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The default is the default address family identifier (AFI) that is set by the **set default-afi** command.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following example shows the output from the **show bfd** command:

```
RP/0/RP0:hostname# show bfd
```

```
IPV4 Sessions Up: 0, Down: 0, Total: 0
```

The following example shows the output from the **show bfd all** command:

```
RP/0/RP0:hostname# show bfd all

IPv4:
-----
IPV4 Sessions Up: 20, Down: 0, Unknown/Retry: 2, Total: 22
IPv6:
-----
IPV6 Sessions Up: 128, Down: 2, Unknown/Retry: 1, Total: 131
Label:
-----
Label Sessions Up: 10, Down: 0, Unknown/Retry: 1, Total: 11
```

show bfd client

To display Bidirectional Forwarding Detection (BFD) client information, use the **show bfd client** command in EXEC mode.

show bfd client [**detail**]

Syntax Description

detail	(Optional) Specifies detailed client information including number of sessions and client reconnects.

Command Default

Enter the **show bfd client** command without specifying the **detail** keyword to display summarized BFD client information.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following example shows the output from the **show bfd client** command:

```
RP/0/RP0:hostname# show bfd client

Name            Node       Num sessions
--------------- ---------- --------------
bgp             0//CPU0 0
isis            0//CPU0 0
isis            0//CPU0 0
```

Table 87: show bfd client Field Descriptions

Field	Description
Name	Name of the BFD client.
Node	Location of the BFD client.

Field	Description
Num sessions	Number of active sessions for the BFD client.

show bfd counters

To display Bidirectional Forwarding Detection (BFD) counter information, use the **show bfd counters** command in EXEC mode.

show bfd counters [{**ipv4** | [{**singlehop** | **multihop**}] | **singlehop**| **all**| **label**}] **packet** [**interface** *type interface-path-id*] **location** *node-id*

Syntax Description

ipv4	(Optional) Displays BFD over IPv4 information only.
singlehop	(Optional) Displays BFD singlehop information only.
multihop	(Optional) Displays BFD multihop information only.
all	(Optional) Displays BFD over IPv4 information.
packet	Specifies that packet counters are displayed.
interface	(Optional) Specifies the interface for which to show counters.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *node-id*	Displays BFD counters from the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The default is the default address family identifier (AFI) that is set by the **set default-afi** command.

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack*/*slot*/*module*/*port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
  - *rack*: Chassis number of the rack.
  - *slot*: Physical slot number of the line card.
  - *module*: Module number. A physical layer interface module (PLIM) is always 0.

- *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Task ID

Task ID	Operations
bgp	read
ospf	read
isis	read
mpls-te	read

Examples

The following example shows the output from the **show bfd counters packet** command for IPv4:

```
RP/0/RP0:hostname# show bfd counters ipv4 packet

IPv4 Singlehop:
 tengige0/0/1/2                  Recv       Xmit                 Recv       Xmit
      Async:                             4148      4137       Echo: (   47136)     80192
tengige0/1/1/2                  Recv       Xmit                 Recv       Xmit
      Async:                             116876    125756       Echo: ( 2268192)   2301312
 Bundle-Ether10                          Recv       Xmit                 Recv       Xmit
      Async:                             2         0       Echo:         0          0
 Bundle-Ether20                          Recv       Xmit                 Recv       Xmit
      Async:                             91         0       Echo:         0          0

IPv4 Multihop: (Src IP/Dst IP/Vrf Id)
 33.15.151.4/33.16.151.4/0x12345678      Recv       Xmit
      Async:                             0       570337
```

show bfd summary

To display the percentage of PPS rate in use per line card, maximum usage of PPS, and total number of sessions, use the **show bfd summary** command in the EXEC mode.

show bfd summary [{**private**}]**location***node-id*

Syntax Description

private	Displays the private information.
location *node-id*	Displays BFD counters from the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific guidelines.

Task ID

Task ID	Operation
bgp	read
ospf	read
isis	read
mpls-te	read

Example

This example shows the sample output from the **show bfd summary** command for a specified location:

```
RP/0/RP0:hostname#show bfd summary location 0/1/cpu0

Node       PPS rate usage  Session number
           %   Used  Max   Total   Max
---------- --------------- --------------
0/1/CPU0   0   80    9600  4       4000
```

This example shows the sample output from the **show bfd summary** command:

```
RP/0/RP0:hostname#show bfd summary
Node       PPS rate usage  Session number
           %   Used  Max   Total   Max
```

```
---------- --------------- --------------
0/0/CPU0   0   0     9600  0       4000
0/1/CPU0   0   0     9600  0       4000
0/2/CPU0   0   0     9600  0       4000
0/5/CPU0   0   0     9600  0       4000
0/6/CPU0   0   0     9600  0       4000
0/7/CPU0   0   0     9600  0       4000
```

Ethernet Local Management Interface Commands

This chapter provides details of the commands used for configuring Ethernet Local Management Interface.

clear ethernet lmi interfaces

To clear Ethernet LMI statistics on one or all interfaces, use the **clear ethernet lmi interfaces** command in EXEC configuration mode.

clear ethernet lmi interfaces {*type interface-path-id* | **all**}

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
all	Specifies clearing of LMI statistics for all Ethernet interfaces running the E-LMI protocol.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Task ID

Task ID	Operation
ethernet-services	execute

The following example shows how to clear E-LMI statistics:

```
RP/0/RP0:hostname# clear ethernet lmi interfaces tengige 0/0/0/0
```

ethernet lmi

To enable Ethernet Local Managment Interface (E-LMI) operation on an interface and enter interface Ethernet LMI configuration mode, use the **ethernet lmi** command in interface configuration mode. To disable Ethernet LMI and return to the default, use the **no** form of the command.

ethernet lmi
no ethernet lmi

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet LMI is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Ethernet LMI is supported only on physical Ethernet interfaces.

Task ID

Task ID	Operation
ethernet-services	read, write

The following example shows how to enable Ethernet LMI on a tengige interface and enter Ethernet LMI configuration mode:

```
RP/0/RP0:hostname# interface tengige 0/1/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if-elmi)#
```

show ethernet lmi interfaces

To display Ethernet Local Management Interface (E-LMI) information for an interface, including protocol status and error and event statistics, use the **show ethernet lmi interfaces** command in EXEC configuration mode.

show ethernet lmi interfaces [*type interface-path-id*][**brief** | **detail**]
show ethernet lmi interfaces [**brief** | **detail**][**location** *location*]

Syntax Description

brief	(Optional) Displays summary information about the E-LMI protocol status, number of EVCs and errors, and CE-VLAN/EVC map type.
detail	(Optional) Displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred, including details about subinterfaces and EVC status.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location *location*	(Optional) Displays E-LMI information for the designated node. The *location* argument is entered in the *rack*/*slot*/*module* notation. **Note** The location cannot be specified when you specify an interface type.

Command Default

The output displays the configured and operational state of E-LMI on the interface, with counts for reliability and protocol errors and elapsed time since various events have occurred since the protocol was enabled on the interface or counters were cleared.

Command Modes

EXEC (#)

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

If Protocol Errors are seen in the output, then the CE device is sending packets to the PE device, but the PE does not understand those packets. This suggests an incorrect implementation of the E-LMI protocol on the

CE side, or corruption of the packets on the path between the CE and PE. E-LMI packets have a strictly defined structure in the MEF 16 standard, and any deviation from that results in a protocol error. The PE will not respond to any packets that are malformed and result in a protocol error.

The Reliability Error counters can indicate that messages are being lost between the PE and CE devices. The timers in the last block of the output should indicate that messages are being sent and received by the PE device. Consider the following actions when these Reliability Errors occur:

- Status Enq Timeouts—If this counter is continuously incrementing, it indicates that the Polling Timer on the CE is configured to a greater value than the PVT configuration on the PE. Status Enquiry messages will be sent less frequently than the PVT expects them and PVT timeouts occur. Be sure that the value of the PVT (specified by the **polling-verification-timer** command on the PE) is greater than the Polling Timer value on the CE device.
- Invalid Sequence Number—Indicates that messages from the PE are not being received by the CE. Be sure that the correct interface on the CE device is connected to the corresponding E-LMI interface on the PE device, so that communication can take place. Verify that both interfaces are Up.
- Invalid Report Type—This error can occur under the following conditions:
  - If the protocol is in the process of a status update and an "E-LMI Check" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.
  - If the protocol is not in the process of a status update and a "Full Status Continued" type of STATUS ENQUIRY is received by the PE, then the PE ignores the ENQUIRY and records an error.

Note If the protocol is in the process of a status update and a "Full Status" type of STATUS ENQUIRY is received by the PE, then the PE restarts the status update but does not record any error.

Task ID

Task ID	Operation
ethernet-services	read

The following example shows sample output for the default form of the command:

```
RP/0/RP0:hostname# show ethernet lmi interfaces
Interface: tengige 0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128

  Reliability Errors:
    Status Enq Timeouts                 19 Invalid Sequence Number            0
    Invalid Report Type                  0

  Protocol Errors:
    Malformed PDUs                       0 Invalid Protocol Version           0
    Invalid Message Type                 0 Out of Sequence IE                 0
    Duplicated IE                        0 Mandatory IE Missing               0
```

```
  Invalid Mandatory IE                0 Invalid non-Mandatory IE            0
  Unrecognized IE                     0 Unexpected IE                       0

Full Status Enq Rcvd     00:00:10 ago   Full Status Sent      00:00:10 ago
PDU Rcvd                 00:00:00 ago   PDU Sent              00:00:00 ago
LMI Link Status Changed  10:00:00 ago   Last Protocol Error      never
Counters cleared            never
```

Table 88: show ethernet lmi interfaces Field Descriptions

Field	Description
Interface:	Name of the interface running the E-LMI protocol.
Ether LMI Link Status:	Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).
UNI Id:	Name of the UNI as configured by the **ethernet uni id** command. This output field does not appear if the UNI ID is not configured.
Line Protocol State:	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
MTU (*x* PDUs reqd for full report)	Maximum Transmission Unit of the interface and the number (*x*) of E-LMI PDUs of that size required to send one full status report.
CE-VLAN/EVC Map Type: *type* (*x* EVCs)	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible valued for *type* are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number *x* of EVCs in the map are displayed in parentheses.
Configuration: Status counter	Value of the MEF N393 Status Counter as configured by the **status-counter** command.
Polling Verification Timer	Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the **polling-verification-timer** command. Displays "disabled" if the PVT is turned off.
Last Data Instance Sent:	Current value of the Data Instance.
Last Sequence Numbers: Sent *x*, Received *y*	Values of the last sent (*x*) and received (*y*) sequence numbers as reported in sent PDUs.

Field	Description
Reliability Errors:	Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared: • Status Enq Timeouts—Increments every time the Polling Verification Timer (PVT) expires. • Invalid Report Type—Increments if the Report Type is not appropriate to the protocol's current state. There are four Report Types defined by the E-LMI Standard, and only three of them can appear in Status Enquiry messages that the PE receives. These are: E-LMI Check, Full Status and Full Status Continued. • Invalid Sequence Number—Increments whenever the received sequence number in a Status Enquiry from the CE does not match the last sent sequence number in the PE response. Indicates that messages from the PE are not being received by the CE. The PE continues to respond with the requested Report Type. For more information about possible actions, see the "Usage Guidelines" section.
Protocol Errors: (Malformed PDUs, Invalid Message Type, Duplicated IE, and others)	Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.
Full Status Enq Rcvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.	Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays "never" if the event has not occurred since the protocol was enabled on the interface or counters were cleared.

The following example shows sample output for the **show ethernet lmi interfaces brief** form of the command:

```
RP/0/RP0:hostname# show ethernet lmi interfaces brief
                     ELMI   LineP      #            CE-VLAN/
Interface            State  State      EVCs  Errors EVC Map
-------------------------------------------------------------------------------
tengige 0/0/0/0            Up     Up            3      19 Multiplexing, no bundling
tengige 0/0/0/1            Down   Admin-down    1       0 All to One Bundling
```

Table 89: show ethernet lmi interfaces brief Field Descriptions

Field	Description
Interface	Name of the interface running the E-LMI protocol.

Field	Description
ELMI State	Status of the E-LMI protocol. Possible values are Up, Down, or N/A if the Polling Verification Timer is disabled.
LineP State	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
# EVCs	Total number of EVCs in the CE-VLAN/EVC map.
Errors	Total number of reliability and protocol errors encountered since the protocol was enabled on the interface or counters were cleared.
CE-VLAN/EVC Map	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible values are Bundling, All to One Bundling, or Multiplexing, no bundling.

The following example shows sample output for the **show ethernet lmi interfaces detail** form of the command:

```
RP/0/RP0:hostname #show ethernet lmi interfaces detail
Interface: tengige 0/0/0/0
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-Slot1-Port0
  Line Protocol State: Up
  MTU: 1500 (2 PDUs reqd. for full report)
  CE-VLAN/EVC Map Type: Bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 1732
  Last Sequence Numbers: Sent 128, Received 128

  Reliability Errors:
    Status Enq Timeouts                19 Invalid Sequence Number             0
    Invalid Report Type                 0

  Protocol Errors:
    Malformed PDUs                      0 Invalid Protocol Version            0
    Invalid Message Type                0 Out of Sequence IE                  0
    Duplicated IE                       0 Mandatory IE Missing                0
    Invalid Mandatory IE                0 Invalid non-Mandatory IE            0
    Unrecognized IE                     0 Unexpected IE                       0

  Full Status Enq Rcvd     00:00:10 ago   Full Status Sent      00:00:10 ago
  PDU Rcvd                 00:00:00 ago   PDU Sent              00:00:00 ago
  LMI Link Status Changed  10:00:00 ago   Last Protocol Error      never
  Counters cleared            never

  Sub-interface: tengige 0/0/0/0.1
    VLANs: 1,10,20-30, default, untagged/priority tagged
    EVC Status: New, Partially Active
    EVC Type: Multipoint-to-Multipoint
    OAM Protocol: CFM
      CFM Domain: Global (level 5)
      CFM Service: CustomerA
    Remote UNI Count: Configured = 2, Active = 1

    Remote UNI Id                                                  Status
```

```
-------------                                                   ------
PE2-CustA-Slot2-Port2                                           Up
PE2-CustA-Slot3-Port3                                           Unreachable
```

Table 90: show ethernet lmi interfaces detail Field Descriptions

Field	Description
Interface:	Name of the interface running the E-LMI protocol.
Ether LMI Link Status:	Status of the E-LMI protocol on the interface. Possible values are Up, Down, or Unknown (PVT disabled).
UNI Id:	Name of the UNI as configured by the **ethernet uni id** command. This output field does not appear if the UNI ID is not configured.
Line Protocol State:	Status of the interface line protocol. Possible values are Up, Down, or Admin-Down.
MTU (*x* PDUs reqd for full report)	Maximum Transmission Unit of the interface and the number (*x*) of E-LMI PDUs of that size required to send one full status report.
CE-VLAN/EVC Map Type: *type* (*x* EVCs)	Map type, which describes how CE VLAN IDs are mapped to specific EVCs. Possible valued for *type* are Bundling, All to One Bundling, or Service Multiplexing with no bundling. The number *x* of EVCs in the map are displayed in parentheses.
Configuration: Status counter	Value of the MEF N393 Status Counter as configured by the **status-counter** command.
Polling Verification Timer	Value of the MEF T392 Polling Verification Timer (in seconds) as configured by the **polling-verification-timer** command. Displays "disabled" if the PVT is turned off.
Last Data Instance Sent:	Current value of the Data Instance.
Last Sequence Numbers: Sent *x*, Received *y*	Values of the last sent (*x*) and received (*y*) sequence numbers as reported in sent PDUs.
Reliability Errors: (Status Enq Timeouts, Invalid Report Type, and Invalid Sequence Number)	Number of times the specified types of reliability errors have occurred since the protocol was enabled on the interface or counters were cleared.
Protocol Errors: (Malformed PDUs, Invalid Message Type, Duplicated IE, and others)	Number of times the specified types of protocol errors have occurred since the protocol was enabled on the interface or counters were cleared.

Field	Description
Full Status Enq Rcvd, PDU Rcvd, LMI Link Status Changed, Counters cleared, Full Status Sent, PDU Sent, and Last Protocol Error.	Elapsed time (hrs:mins:secs ago) since the specified events last occurred or counters were cleared. Displays "never" if the event has not occurred since the protocol was enabled on the interface or counters were cleared.
Subinterface:	Name of the subinterface corresponding to the EVC.
VLANs:	VLAN traffic on the interface that corresponds to the EFPs encapsulation, with the following possible values: • Numbers of the matching VLAN IDs **Note** If Q-in-Q encapsulation is configured, only the outer tag is displayed. • default—Indicates that Default tagging is configured, or the encapsulation specifies to match "any." • none—No matches for the configured encapsulation have occurred on the interface. • untagged/priority—Traffic is either untagged or has priority tagging. **Note** If the message "EVC omitted from Full Status due to encapsulation conflict" is displayed above the VLAN output, a misconfiguration has occurred with two or more EFPs having a conflicting encapsulation.
EVC Status:	State of the EVC, with the following possible values: • Active—E-LMI is operational for this EVC. • Inactive—All of the remote UNIs are unreachable or down. • New—The EVC has not yet been reported to the CE device. • Not yet known—E-LMI is still waiting to receive the status from CFM. This condition should not persist for more than a few seconds. • Partially Active—One or more of the remote UNIs is unreachable or down.
EVC Type:	Type of the EVC, with the following possible values: "Point-to-Point," "Multipoint-to-Multipoint," or "EVC type not yet known."

Field	Description
OAM Protocol:	The OAM protocol from which the EVC status and type are derived. Possible values are either "CFM" or "None."
CFM Domain:	Name of the CFM domain for this EVC.
CFM Service:	Name of the CFM service for this EVC.
Remote UNI Count: Configured = *x*, Active = *y*	Number of configured or expected remote UNIs (*x*) and the number of active remote UNIs (*y*) within the EVC.
Remote UNI Id:	ID of each remote UNI, including both configured and active remote UNIs where these two sets are not identical. If the number of configured and active remote UNIs is zero, no table is displayed. **Note** Where no ID is configured for a remote UNI using the **ethernet uni id** command, then the CFM remote MEP ID is displayed, for example, "<Remote UNI Reference Id: *x*>"
Status	Status of each remote UNI, with the following possible values: "Up," "Down," "Admin Down," "Unreachable (a configured remote UNI is not active or missing)," or "Unknown (a remote UNI is active but not reporting its status)."

Inter-Rack Pairing Command Reference

This chapter describes the commands to configure Inter-Rack Pairing.

sdr default-sdr pairing-mode inter-rack

To enable pairing of RPs between racks in secure domain routers (SDRs), use the **sdr default-sdr pairing-mode inter-rack** command in the appropriate mode. The inter-rack mode of pairing provides high availability against rack failures.

sdr default-sdr pairing-mode inter-rack

Syntax Description

pairing-mode	Specifies the pairing-mode of RPs.
inter-rack	Enables the pairing of RPs between racks.

Command Default

A single SDR named **default-sdr** is configured on the router.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Usage Guidelines

Inter-rack pairing is applicable only in a multi chassis configuration.

Example

This example shows how to use the **sdr default-sdr pairing-mode inter-rack** command:

```
RP/0/RP0:hostname# sdr default-sdr pairing-mode inter-rack
```

sdr default-sdr re_pair

To initiate re-pairing of RPs in the currently defined secure domain routers (SDRs), use the **sdr default-sdr re_pair** command in the appropriate mode.

sdr default-sdr re_pair

Syntax Description

re_pair	Activates the re-pairing of RPs in the defined SDR.

Command Default

None

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Usage Guidelines

None

Example

This example shows how to use the **sdr default-sdr re_pair** command:

```
RP/0/RP0:hostname # sdr default-sdr re_pair
```

show default-sdr sdr-pairing

To display information about the pairing details of the currently defined secure domain routers (SDRs), use the **show default-sdr sdr-pairing** command in the appropriate mode.

show sdr-default sdr-pairing

Syntax Description

sdr-pairing	Displays the current pairing of the RPs.

Command Default

A single SDR named **default-sdr** is configured on the router.

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.5.25	This command was introduced.

Usage Guidelines

None

Example

This example shows how to use the **show default-sdr sdr-pairing** command:

```
RP/0/RP0:hostname# show default-sdr sdr-pairing

Pairing Mode  INTER-RACK  SDR Lead
   Node 0 0/RP1
   Node 1 1/RP0
 Pairs
   Pair Name Pair0
    Node 0   0/RP1
    Node 1   1/RP0
 Pairs
   Pair Name Pair1
    Node 0   1/RP1
    Node 1   2/RP0
 Pairs
   Pair Name Pair2
    Node 0   2/RP1
    Node 1   3/RP0
 Pairs
   Pair Name Pair3
    Node 0   3/RP1
    Node 1   0/RP0
```

Smart Licensing Command Reference

This chapter describes the commands to configure smart licensing.

license smart deregister

To cancel the registration of your device, use the **license smart deregister** command.

license smart deregister

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

When your device is taken off the inventory, shipped elsewhere for redeployment or returned to Cisco for replacement using the return merchandise authorization (RMA) process, you can use this command to cancel the registration on your device. All smart licensing entitlements and certificates on the platform are removed.

The following example deregisters the NCS 4000 router :

```
RP/0/RP0:hostname# license smart deregister
```

license smart register

To register the device instance with the Cisco licensing cloud, use the **license smart register idtoken** *token-id* **force** command.

license smart register idtoken *token-id* **force**

Syntax Description

token_id	Specifies the token generated in smart manager.
force	If the registration fails due to communication failure between the device and the portal or satellite, CTC waits for 24 hours before attempting to register the device again. Use this option to force the registration.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

Use this command to register the device instance with the Cisco licensing cloud.

The following example registers and sets the token ID required for registration of the NCS 4000 router :

```
RP/0/RP0:hostname# license smart register token-id
```

license smart renew

To manually renew the ID certification or authorization, use the **license smart renew** command.

license smart renew id { **ID|auth]** }

Syntax Description

ID	ID certificates are renewed automatically after six months. In case, the renewal fails, the product instance goes into unidentified state. You can manually renew the ID certificate using this option.
auth	Authorization periods are renewed by the Smart Licensing system every 30 days. As long as the license is in an 'Authorized' or 'Out-of-compliance' (OOC), the authorization period is renewed. Use this command to make an on-demand manual update of your registration. Thus, instead of waiting 30 days for the next registration renewal cycle, you can use this option to instantly find out the status of your license. After 90 days, the authorization period expires and the status of the associated licenses display "AUTH EXPIRED". Use this option to retry the authorization period renewal. If the retry is successful, a new authorization period begins.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

None

The following example manually renews the ID certificate for the NCS 4000 router :

```
RP/0/RP0:hostname# license smart renew id
```

The following example manually renews the authorization for the NCS 4000 router :

```
RP/0/RP0:hostname# license smart renew auth
```

show alarms

To display alarms related to the system, use the **show alarms** command.

show alarms brief system active force

Syntax Description

brief	Displays alarms in brief.
system	Displays system scope alarms related data.
active	Displays active alarms.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following example displays the output of the show alarms brief system active command:

```
RP/0/RP0:hostname# show alarms brief system active
Fri Jun  9 14:21:20.143 UTC

------------------------------------------------------------------------------------
Active Alarms
------------------------------------------------------------------------------------
Location        Severity     Group            Set Time                    Description



------------------------------------------------------------------------------------
0               Major        Environ          06/01/2017 17:58:15 UTC    Power Shelf
redundancy lost.

0/RP0           Minor        Fabric           06/01/2017 18:00:13 UTC    Fabric Plane-3 is
 Down

0               Major        Shelf            06/01/2017 18:00:32 UTC    Fabric Card
Redundancy Lost

0/RP0           Major        FPD_Infra        06/06/2017 09:18:38 UTC    One Or More FPDs
Need Upgrade Or Not In Current State

0/RP1           Major        FPD_Infra        06/06/2017 09:18:38 UTC    One Or More FPDs
Need Upgrade Or Not In Current State
```

```
0/9             Major        FPD_Infra        06/06/2017 09:25:23 UTC    One Or More FPDs
Need Upgrade Or Not In Current State

0/9             Minor        Controller       06/06/2017 09:25:33 UTC    Optics0/9/0/0 -
Port Pluggable Module Mismatched With Pre-Provisoned PPM

0/9             Minor        Controller       06/06/2017 09:25:33 UTC    Optics0/9/0/1 -
Improper Removal

0/9             Minor        Controller       06/06/2017 09:25:34 UTC    Optics0/9/0/11 -
Improper Removal

0/RP0           NotReported  Software         06/09/2017 10:55:51 UTC    One Or More
Entitlements Are Out Of Compliance
0/RP0           NotReported  Software         06/09/2017 14:16:29 UTC    Communications
Failure With Cisco Licensing Cloud
```

show license all

To view the entitlements in use, use the **show license all** command.

show license all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following example displays all entitlements in use. It can also be used to check if Smart Licensing is enabled. Additionally, it shows associated licensing certificates, compliance status, UDI, and other details for the NCS 4000 router:

```
 RP/0/RP0:hostname# show license all
 Wed Jun  7 11:18:35.953 UTC

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: NCS4K
  Virtual Account: Default
  Initial Registration: SUCCEEDED on Fri Jun 02 2017 14:27:19 UTC
  Last Renewal Attempt: SUCCEEDED on Fri Jun 02 2017 14:56:40 UTC
    Failure reason:
  Next Renewal Attempt: Wed Nov 29 2017 14:56:41 UTC
  Registration Expires: Sat Jun 02 2018 09:29:55 UTC

License Authorization:
  Status: AUTHORIZED on Tue Jun 06 2017 09:53:03 UTC
  Last Communication Attempt: FAILED on Tue Jun 06 2017 09:53:03 UTC
    Failure reason: Fail to send out Call Home HTTP message
  Next Communication Attempt: Thu Jul 06 2017 04:16:31 UTC
  Communication Deadline: Mon Sep 04 2017 04:16:31 UTC

License Usage
==============

 NCS 4000 400G Packet/OTN/WDM - QSFP28/CFP2 - Lic. 100G OTN (NCS4K-4H-OPW-LO):
  Description: NCS 4000 400G Packet/OTN/WDM - QSFP28/CFP2 - Lic. 100G OTN
```

```
  Count: 1
  Version: 1.0
  Status: PENDING

 NCS4K 100G Bandwidth Licenses (S-NCS4K-100G-LIC):
  Description: NCS4K 100G Bandwidth Licenses
  Count: 2
  Version: 1.0
  Status: PENDING

 SW License for WDM CFP2 Pluggable port (S-CFP2-WDM-LIC):
  Description: SW License for WDM CFP2 Pluggable port
  Count: 1
  Version: 1.0
  Status: PENDING

Product Information
===================
UDI: SN:SAL1834Z18D,UUID:default-sdr
HA UDI List:
    Active:SN:SAL1834Z18D,UUID:default-sdr
    Standby:SN:SAL1834Z18D,UUID:default-sdr

Agent Version
=============
Smart Agent for Licensing: 2.2.0_rel/30
```

show license status

To display the registration details, status of license, and authorization details of license, use the **show license status** command.

show license status

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following example displays the output of the show license status command:

```
 RP/0/RP0:hostname# show license status
Wed Jun  7 05:42:22.392 UTC
Smart Licensing is ENABLED
  Initial Registration: SUCCEEDED on Wed Jun 07 2017 12:06:50 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mon Dec 04 2017 12:07:10 UTC
  Registration Expires: Thu Jun 07 2018 06:40:34 UTC

License Authorization:
  Status: AUTHORIZED on Wed Jun 07 2017 12:07:50 UTC
  Last Communication Attempt: SUCCEEDED on Wed Jun 07 2017 12:07:50 UTC
  Next Communication Attempt: Fri Jul 07 2017 12:07:49 UTC
  Communication Deadline: Tue Sep 05 2017 06:41:16 UTC
```

show license summary

To display the license summary, use the **show license summary** command.

show license summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following example displays the output of the show license summary command:

```
 RP/0/RP0:hostname# show license summary
 Fri Jun  9 15:53:53.301 UTC

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: NCS4K
  Virtual Account: NCS4K-VIRTUAL-AC
  Last Renewal Attempt: None
  Next Renewal Attempt: Wed Dec 06 2017 15:51:48 UTC

License Authorization:
  Status: OUT OF COMPLIANCE on Fri Jun 09 2017 15:53:08 UTC
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Sat Jun 10 2017 03:53:08 UTC

License Usage:
  License             Entitlement tag          Count  Status
  -----------------------------------------------------------
  NCS 4000 400G Packet/OTN/WDM - QSFP28/CFP2 - Lic. 100G OTN(NCS4K-4H-OPW-LO)           1
  OUT OF COMPLIANCE
  NCS4K 100G Bandwidth Licenses(S-NCS4K-100G-LIC)          2   OUT OF COMPLIANCE
  SW License for WDM CFP2 Pluggable port(S-CFP2-WDM-LIC)            1   OUT OF COMPLIANCE
```

Call Home Command Reference

This chapter describes the commands to configure call home.

active

To enable a Call Home profile, use the **active** command.

active

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Call home profile configuration mode

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

You must enable a profile using the active command so that call home messages can be triggered.

The following example shows how to activate a profile:

```
 RP/0/RP0:hostname# configure
  RP/0/RP0:hostname(config)# call-home
RP/0/RP0:hostname(config-call-home)# profile my-profile
RP/0/RP0:hostname(config-call-home-profile)# active
```

destination address

To specify an email address to which Call Home messages are sent, use the **destination address** command.

destination address *email-address*

Syntax Description

email address	Specifies the email address to which call home messages can be sent.

Command Default

None

Command Modes

Call home profile configuration mode

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

You must define a destination email address to send out Call Home messages.

The following example shows how to configure the destination email address:

```
 RP/0/RP0:hostname# configure
  RP/0/RP0:hostname(config)# call-home
RP/0/RP0:hostname(config-call-home)# profile my-profile
RP/0/RP0:hostname(config-call-home-profile)# destination address email support-me@cisco.com
```

destination transport-method

To specify the transport method for Call Home messages for a specific profile, use the **destination transport-method** command.

destination transport-method [email |http]

Syntax Description

email	Enables an e-mail address for the profile.
http	Enables an HTTP URL for the profile.

Command Default

None

Command Modes

Call home profile configuration mode

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

For the user profile, both e-mail and http can be enabled. For the Cisco TAC profile, only one transport method can be enabled.

The following example shows how to configure the transport method to be email:

```
 RP/0/RP0:hostname# configure
  RP/0/RP0:hostname(config)# call-home
RP/0/RP0:hostname(config-call-home)# profile my-profile
RP/0/RP0:hostname(config-call-home-profile)# destination transport-method email
```

http-proxy

To configure the Call Home HTTP proxy server, use the **http-proxy** command.

http-proxy *proxy-server-name* **port** *port-number*

Syntax Description

proxy-server-name	Specifies the name of the proxy server.
port-number	Specifies the port for the specified HTTP proxy server.

Command Default

None

Command Modes

Call home profile configuration mode

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

None

The following example configures the call home HTTP proxy server :

```
 RP/0/RP0:hostname# configure
  RP/0/RP0:hostname(config)# call-home
RP/0/RP0:hostname(config-call-home)# http-proxy aa.bbb.cc.dd port 100
```

show call-home profile

To display the Call Home profiles, use the **show call-home profile** command.

show call-home profile { **all** |*profile-name* }

Syntax Description

all	Displays information for all profiles.
profile-name	Specifies the name of the profile for which to display information.

Command Default

None

Command Modes

none

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

None

The following example shows sample output from the show call-home profile command:

```
RP/0/RP0:hostname# show call-home profile all
 Tue Aug 29 15:17:11.965 UTC


Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
    Other address(es): callhome@cisco.com


    Periodic configuration info message is scheduled every 16 day of the month at 12:42

    Periodic inventory info message is scheduled every 16 day of the month at 12:27

    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        critical

Profile Name: test
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
```

```
Transport Method: email and http
HTTP  address(es): Not yet set up
Email address(es): Not yet set up

Alert-group               Severity
------------------------  ------------
N/A                       N/A

Syslog-Pattern            Severity
------------------------  ------------
N/A                       N/A
```

show call-home smart-licensing

To display smart licensing information for the Call Home profiles, use the **show call-home smart-licensing** command.

show call-home smart-licensing

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

none

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

None

The following example shows sample output from the show call-home smart-licensing command:

```
 RP/0/RP0:hostname# show call-home smart-licensing
  Tue Aug 29 14:48:39.406 UTC
Current smart-licensing transport settings:
Smart-license messages: enabled
Profile: CiscoTAC-1 (status: ACTIVE)
Destination  URL(s):  https://tools.cisco.com/its/service/oddce/services/DDCEService
```

show call-home smart-licensing statistics

To display the Call Home smart licensing statistics, use the **show call-home smart-licensing statistics** command.

show call-home smart-licensing statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

none

Command History

Release	Modification
Release 6.1.32	This command was introduced.

Usage Guidelines

None

The following example shows sample output from the show call-home smart-licensing statistics command:

```
 RP/0/RP0:hostname# show call-home smart-licensing statistics
 Tue Aug 29 14:48:50.001 UTC
Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.

Msg Subtype      Success Failed  Inqueue Dropped Last-sent (GMT+00:00)
-------------------------------------------------------------------------
ENTITLEMENT      99      0       0       0       2017-08-29 12:22:03
DEREGISTRATION   12      0       0       0       2017-08-29 12:07:30
REGISTRATION     16      66      0       0       2017-08-29 12:20:28
ACKNOWLEDGEMENT  15      0       0       0       2017-08-29 12:20:36
RENEW            2       0       0       0       2017-08-22 14:48:45
```

System Upgrade Command Reference

This chapter provides details for the commands used in In-Service System Upgrade (ISSU) and Orchestrated Line Card Reload (OLR).

hardware-module olr

To divide the line cards on to two planes while preparing the node for OLR, use the **hardware-module olr** command in the global configuation mode.

hardware-module olr plane *plane-id***rack** *rack-id* **nodes** *node/ lc-list*

Syntax Description

plane *plane-id*	Specifies the plane. The line cards can be divided on to plane A or plane B.
rack *rack-id*	Specifies the rack in which the line card is present.
nodes *node/ lc-list*	Specifies the node of the line card.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Example

The following example shows how to use the hw-module olr command:

```
RP/0/RP0:hostname(config) # hw-module plane A rack 0 nodes 1,2,3
```

install activate

To enable the package configurations to be made active on the router so new features and software fixes take effect, use the **install activate** command in EXEC mode or Admin EXEC mode.

install activate *package_name*

Syntax Description

package_name	Enter the package name separated by space. Up to 16 packages can be specified in a single **install activate** command at a time.

Command Default

The **install activate** command activates all packages that were added in the specified install add operation and the operation is performed in an asynchronous mode. The command runs in the background and the EXEC prompt is returned soon after.

Command Modes

Admin EXEC, EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Only the inactive packages can be activated. Use the **show install inactive** command to identify the inactive packages present in the repository.

Example

The following example shows how to use the install activate command:

```
sysadmin-vm:0_RP0#install activate ncs4k-sysadmin-6.1.4.40I
```

install add

To copy the contents of a package installation envelope (PIE) to a storage device, use the **install add** command in Admin EXEC or EXEC mode.

install add source *source-path file***[issu]**

Syntax Description

source *source-path*	Specifies the source location of the PIE files to be appended to the PIE filenames. Location options are: • **disk0:** • **disk1:** • **compact flash:** • **harddisk** • **ftp://** • **tftp://**
file	Name and location of the PIE file to be installed.
issu	Performs an in-service software upgrade.

Command Default

Packages are added to the storage device. The **install add** command runs in the background and the EXEC prompt is returned as soon as possible.

Command Modes

EXEC, Admin EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

Use the **install add** command to unpack the package software files from a PIE file and copy them to the boot device (usually disk0:). You can also use ftp, tftp, or sftp protocols to transfer files from the network server to the router.

Example

The following example shows how to use the install add command:

```
sysadmin-vm:0_RP0#install add source tftp://223.255.254.254/auto/tftp
```

install extract

To extract individual ISO images from main ISO package and place the installable files in the repository, use the **install extract** command in the System Admin EXEC or XR EXEC mode.

install extract *package_name*

Syntax Description

package_name	Enter package names separated by space.

Command Default

None

Command Modes

EXEC, System EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Example

The following example shows how to use the install extract command:

```
sysadmin-vm:0_RP0#install extract ncs4k-mini-x-6.1.4.09I
```

install prepare

To prepare the installable files (ISO image, packages and SMUs) for activation using ISSU , use the **install prepare** command in the System Admin EXEC or XR EXEC mode. This command performs pre-activation checks and the loads individual components of the installable files on to the router setup. The advantage of preparing the installable files is that the time required for subsequent activation is considerably reduced.

install prepare issu *package_name*

Syntax Description

package_name	Enter package names separated by space.

Command Default

None

Command Modes

System Admin EXEC, EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Example

The following example shows how to use the install prepare command:

```
sysadmin-vm:0_RP0#install prepare issu ncs4k-sysadmin-6.1.4.40I
```

show install repository

To display the packages in the repository, use the **show install repository** command in the System Admin EXEC or XR EXEC mode.

show install repository [all]

Syntax Description

all	Displays the ISO images, SMUs, and software packages present in the software repository of all VMs.

Command Default

None

Command Modes

System Admin EXEC, EXEC

Command History

Release	Modification
Release 6.1.42	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Example

The following example shows how to use show install respository command:

```
sysadmin-vm:0_RP1# show install repository all
```

save configuration database

To back up the contents of persistent configuration commit database and ifindexes into a backup file, use the **save configuration database** command. This command helps to restore a device with the same configuration and ifindexes later.

save configuration database *filename*

Syntax Description

filename	Name of the tar file where persistent configuration commit database and ifindexes are stored.

Command Default

None

Command Modes

Exec mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

- User should be part of config-services task ID.
- Command can only be executed from DLRSC node.

Example

This example shows how to use the **save configuration database** command:

```
RP/0/RP0:R4#save configuration database samplebackup
Configuration database successfully backed up at: /harddisk:/ samplebackup.tgz
```

restore configuration database

To restore the saved configuration and ifindexes from the specified tar file, use the **restore configuration database** command. This command boots the system with the configuration and ifindexes present in the back-up file. Also, this command triggers an automatic reload of the router.

restore configuration database *filename*

Syntax Description

filename	Name of the tar file from where persistent configuration database and ifindexes are restored.

Command Default

None

Command Modes

Exec mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

- User should be part of config-services task ID.
- Command can only be executed from DLRSC node.

Example

This example shows how to use the **restore configuration database** command:

```
RP/0/RP0:ios#restore configuration database samplebackup.tgz
Tue Jun  1 11:25:04.869 UTC

Restore DB will result in router reload. Do you wish to continue?? [no]: yes
Sync Active RP List
Sync Active RP List
RP/0/RP0:Jun  1 11:25:24.604 UTC: sysmgr_control[69132]: %OS-SYSMGR-4-PROC_SHUTDOWN_NAME :
 User root (UNKNOWN) requested a shutdown of process cfgmgr-rp at all nodes
RP/0/RP0:Jun  1 11:25:24.867 UTC: sysmgr_control[69148]: %OS-SYSMGR-4-PROC_SHUTDOWN_NAME :
 User root (UNKNOWN) requested a shutdown of process ifindex_server at all nodes
Reloading in 10 seconds.
Reloading in 9 seconds.
Reloading in 8 seconds.
Reloading in 7 seconds.
Reloading in 6 seconds.
Reloading in 5 seconds.
Reloading in 4 seconds.
Reloading in 3 seconds.
Reloading in 2 seconds.
Reloading in 1 seconds.
nohup: appending output to `/disk0:/nohup.out'
Configuration database restore will start
LC/0/LC0:Jun  1 11:28:44.208 UTC: rmf_svr[255]: %HA-REDCON-1-STANDBY_NOT_READY : standby
card is NOT ready
LC/0/LC0:Jun  1 11:28:46.709 UTC: rmf_svr[255]: %PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR
:RP-RED-LOST-NNR :DECLARE :0/LC0:
0/RP1/ADMIN0:Jun  1 11:29:00.876 UTC: vm_manager[3343]: %INFRA-VM_MANAGER-4-INFO : Info:
```

```
vm_manager brought down VM default-sdr--2
0/RP0/ADMIN0:Jun  1 11:29:10.526 UTC: vm_manager[3354]: %INFRA-VM_MANAGER-4-INFO : Info:
vm_manager brought down VM default-sdr--2
0/RP1/ADMIN0:Jun  1 11:29:12.749 UTC: vm_manager[3343]: %INFRA-VM_MANAGER-4-INFO : Info:
vm_manager started VM default-sdr--2
RP/0/RP0:Jun  1 11:29:16.508 UTC: rmf_svr[209]: %HA-REDCON-1-STANDBY_NOT_READY : standby
card is NOT ready
RP/0/RP0:Jun  1 11:29:19.011 UTC: rmf_svr[209]: %PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR
:RP-RED-LOST-NNR :DECLARE :0/RP0:
RP/0/RP0:Jun  1 11:29:19.035 UTC: rmf_svr[209]: %PKT_INFRA-FM-2-FAULT_CRITICAL :
ALARM_CRITICAL :RP-RED-LOST-PNP :DECLARE :0/RP0:
RP/0/RP0:Jun  1 11:29:19.037 UTC: rmf_svr[209]: %PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR
:RP-RED-LOST-NSRNR :DECLARE :0/RP0:
0/RP0/ADMIN0:Jun  1 11:29:22.105 UTC: vm_manager[3354]: %INFRA-VM_MANAGER-4-INFO : Info:
vm_manager started VM default-sdr--2
```

show redundancy

To display the status of route processor redundancy, use the **show redundancy** command in System Admin EXEC or EXEC mode.

show redundancy [summary]

Syntax Description

summary	Displays a summary of all redundant node pairs in the router.

Command Default

None

Command Modes

EXEC, System EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Example

The following example shows how to use the show redundancy summary command for single chassis system:

```
RP/0/RP0:R1 #show redundancy summmary
Active Node Standby Node
----------- ------------
0/RP0 0/RP1 (Node Ready, NSR:Ready)
0/LC0 0/LC1 (Node Ready, NSR:Not Configured)
```

This command checks the current status of the RP1 and RP0.

The following example shows how to use the show redundancy summary command for multi chassis system:

```
RP/0/RP0:R1#show redundancy summary
Active Node Standby Node
----------- ------------
1/LC0 1/LC1 (Node Ready, NSR:Not Configured)
0/RP1 2/RP0 (Node Ready, NSR:Not Configured)
3/LC0 3/LC1 (Node Ready, NSR:Not Configured)
0/RP0 1/RP1 (Node Ready, NSR:Not Configured)
2/RP1 3/RP0 (Node Ready, NSR:Ready)
0/LC0 0/LC1 (Node Ready, NSR:Not Configured)
1/RP0 3/RP1 (Node Ready, NSR:Not Configured)
2/LC0 2/LC1 (Node Ready, NSR:Not Configured)
```

show processes

To display information about active processes, use the **show processes** command in System Admin EXEC, or EXEC mode.

show processes { process-name | location *node id* **}**

Syntax Description

process-name	Process name for which all simultaneously running instances are displayed, if applicable
location *node-id*	Displays information about the active processes from a designated node.

Command Default

None

Command Modes

System Admin EXEC, EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

No specific usage guidelines.

Example

The following example shows how to use the show processes command:

```
show processes shelf_mgr location 3/RP0
Fri Jan 24 07:27:49.529 UTC
------------------------------------------------------------------------
PID: 3327
Executable path:
/opt/cisco/calvados/packages/ncs4k-sysadmin-system-6.5.26.CSCvp28576.all-1.0.0/bin/shelf_mgr
Instance #: 0
Respawn: ON
Respawn count: 1
Max. spawns per 4 mins: 4
Last started: 01/24/2020 05:37:36.000
Process state: Run
startup_path:
/opt/cisco/calvados/packages/ncs4k-sysadmin-system-6.5.26.CSCvp28576.sc-1.0.0/etc/startup/shelf_mgr_rp.startup
Ready: 3s
Table of services hosted on this process:
------------------------------------------------------------------------
LAST STARTED SCOPE SELE- ROLE STATE HA- SERVICE NAME
CTED RDY
------------------------------------------------------------------------
01/24/2020 05:41:17.000 RACK Y ACT Run RM
01/24/2020 06:48:49.000 SYS Y ACT Run SM
----------------------
```

install commit

To commit the newly activated software, use the **install commit** command in System Admin EXEC, or EXEC mode.

install commit

Command Default None

Command Modes System Admin EXEC, EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines None

Example

The following example shows how to use the install commit command:

```
sysadmin-vm:0_RP0# install commit
result Mon Jan 21 00:41:32 2020 Install operation 78 (install commit) started by user 'root'
 will
continue asynchronously.
sysadmin-vm:0_RP0# Tue Jan 21 00:41:36 2020 Install operation 78 completed successfully.
sysadmin-vm:0_RP0#
```

Priority Shutdown Commands

This chapter provides details of the commands used for assigning priorities to the line cards for shutdown.

power-mgmt progressive location

To enable the LC priority shutdown feature on the chassis, use the **power-mgmt progressive location** command in the global configuration mode.

power-mgmt progressive location *rack-id*

Syntax Description

rack-id	The ID of the rack.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

None

Example

The following example enables the LC priority shutdown on the chassis specified.

```
RP/0/RP0:hostname (config)#power-mgmt progressive location L0
```

priority location

To configure the shutdown priority to the line card specified, use the **priority location** command in the power-mgmt progressive configuration mode.

priority location *line-card-location card-priority*

Syntax Description

line-card-location	The ID of the rack and slot.
card-priority	The shutdown priority.

Command Default

None

Command Modes

Power-mgmt progressive configuration mode.

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

None

Example

The following example configures the shutdown priority to the line card specified.

```
RP/0/RP0:hostname (config-location-L0)#priority location 0/9 6
```

ACL Commands

This chapter provides details of the commands used for configuring access control lists (ACL).

ipv4 access-group

To configure the Access List (ACL), use the **ipv4 access-group** command at the IPv4 interface in the interface configuration mode.

ipv4 access-group *access-list-name* **ingress**

Syntax Description

access-list-name	Access list name. Names cannot contain a space or quotation marks.
ingress	Specifies an inbound interface.

Command Default

No IPv4 access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

Use the **ipv4 access-list** command to configure an IPv4 access list. This command places the system in access list configuration mode, in which the denied or permitted access conditions must be defined with the deny or permit command.

Example

The following examples shows how to configure the Access List at the IPv4 interface in the configuration mode:

```
interface MgmtEth0/RP0/EMS/0
ipv4 address 5.5.5.1 255.255.255.0
ipv4 access-group EMS ingress
!
ipv4 access-list EMS
10 permit udp any any
!
```

Sample Configuration for IPv4 Access Lists

```
ipv4 access-list CRAFT
10 deny icmp any any
ipv4 access-list EMS
10 deny icmp any any (200 matches)
```

ipv6 access-group

To configure the Access List (ACL), use the **ipv6 access-group** command at the IPv6 interface in the interface configuration mode.

ipv6 access-group *access-list-name* **ingress**

Syntax Description

access-list-name	Access list name. Names cannot contain a space or quotation marks.
ingress	Specifies an inbound interface.

Command Default

No IPv6 access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

Use the ipv6 access-list command to configure an IPv6access list. This command places the system in access list configuration mode, in which the denied or permitted access conditions must be defined with the deny or permit command.

Example

The following examples shows how to configure the Access List at the IPv6 interface in the configuration mode

```
interface MgmtEth0/RP0/EMS/0
ipv6 address 2001:db8::1/64
ipv6 access-group EMS ingress
!
ipv6 access-list EMS
10 permit udp any any
!
```

Sample Configuration for IPv6 Access Lists

```
ipv6 access-list CRAFT
10 deny icmp any any
ipv6 access-list EMS
10 deny icmp any any (200 matches)
```

show access-lists ipv4

To display the contents of current IPv4 access lists, use the **show access-lists ipv4** command in EXEC mode.

show access-lists ipv4 [**interface MgmtEth** *R/S/I/P* | **maximum** [**detail**] | **summary** [*access-list-name*] | **usage pfilter location** { **location** *node-id* | **all** } | *access-list-name* [*sequence-number* | **usage pfilter location** { **location** *node-id* | **all** }]]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port/ number of the interface.
access-list-name	(Optional) Name of a particular IPv4 access list. The name cannot contain a space or quotation mark; it may contain numbers.
location *number*	Location of a particular IPv4 access list.
location*node-id*	(Optional) Location of a particular IPv4 access list. The node-id argument is entered in the rack/slot/module notation.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
summary	Displays a summary of all current IPv4 access lists.
sequence-number	(Optional) Sequence number of a particular IPv4 access list.
maximum	Displays the current maximum number of configurable IPv4 accesscontrol lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv4 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

Use the **show access-lists ipv4** command to display the contents of all IPv4 access lists. To display the contents of a specific IPv4 access list, use the name argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **show access-lists ipv4 summary** command to display a summary of all current IPv4 access lists. To display a summary of a specific IPv4 access list, use the name argument.

Use the **show access-lists ipv4 maximum detail** command to display the OOR details for IPv4 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

Example

In the following example, the contents of all IPv4 access lists are displayed:

RP/0/RP0/CPU0:ios# **show access-lists ipv4**

```
ipv4 access-list CRAFT
10 deny icmp any any
ipv4 access-list EMS
10 deny icmp any any (200 matches)
```

RP/0/RP0/CPU0:ios# **show access-lists test_ro_traffic_generic**

```
Mon Jun 28 15:32:39.456 IST
ipv4 access-list test_RO_Traffic_Generic
10 permit tcp 100.1.0.0 0.0.255.255 eq bgp 100.1.0.0 0.0.255.255
20 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq bgp
30 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq 6784
40 permit udp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
50 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
60 permit tcp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
70 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
80 permit icmp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255
87 deny udp host 12.12.12.1 32.32.32.240 0.0.0.15 eq snmp
```

show access-lists ipv6

To display the contents of current IPv6 access lists, use the **show access-lists ipv6** command in EXEC mode.

show access-lists ipv6 [**interface MgmtEth** *R/S/I/P* | **maximum** [**detail**] | **summary** [*access-list-name*] | **usage pfilter location** { **location** *node-id* | **all** } | *access-list-name* [*sequence-number* | **usage pfilter location** { **location** *node-id* | **all** }]]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port/ number of the interface.
access-list-name	(Optional) Name of a particular IPv6 access list. The name cannot contain a space or quotation mark; it may contain numbers.
location *number*	Location of a particular IPv6 access list.
location *node-id*	(Optional) Location of a particular IPv6 access list. The node-id argument is entered in the rack/slot/module notation.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
summary	Displays a summary of all current IPv6 access lists.
sequence-number	(Optional) Sequence number of a particular IPv6 access list.
maximum	Displays the current maximum number of configurable IPv6 accesscontrol lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv6 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

The **show access-lists ipv6** command is similar to the **show access-lists ipv4** command, except that it is IPv6 specific.

Use the **show access-lists ipv6** command to display the contents of all IPv6 access lists. To display the contents of a specific IPv6 access list, use the name argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **show access-lists ipv6 summary** command to display a summary of all current IPv6 access lists. To display a summary of a specific IPv6 access list, use the name argument.

Use the **show access-lists ipv6 maximum detail** command to display the OOR details for IPv6 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

Example

In the following example, the contents of all IPv6 access lists are displayed:

RP/0/RP0/CPU0:ios#**show access-lists ipv6**

```
RP/0/RP0:hostname#show access-lists ipv6
ipv6 access-list CRAFT
10 deny icmp any any
ipv6 access-list EMS
10 deny icmp any any (200 matches)
```

PTP Commands

This chapter describes the commands used to configure the Precision Time Protocol (PTP).

announce

To configure options for configuring PTP profile announcement messages, use the **announce** command in PTP profile configuration mode.

announce frequency *frequency*

Syntax Description

frequency *frequency*	Use to specify multiple announce messages per second (2, 4, 8, 16, 32, 64, or 128). Frequency of 4 means that four messages are sent per second.

Command Default

No default behavior or values.

Command Modes

PTP profile configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example shows how to sets the announcement frequency to 8 seconds in the PTP configuration profile.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# profile p1
RP/0/RP0/CPU0:router(config-ptp-profile)# announce frequency 8
```

clock profile

To configure the ITU-T Telecom profile and clock type that can be used in all local PTP sessions, use the **clock profile** command in the PTP configuration mode.

clock profile g.8275.1 clock-type T-BC

Syntax Description

clock-type T-BC	Indicates the clock type for G.8275.1 profile. G.8275.1 profile supports T-BC (Telecom Boundary Clock)

Command Default

The default PTP profile defined in the IEEE-1588 standard is used if this configuration is not used.

Command Modes

PTP configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example shows configuring G.8275.1 profile with T-BC clock type:

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# clock
RP/0/RP0/CPU0:router(config-ptp-clock)# domain 24
RP/0/RP0/CPU0:router(config-ptp-clock)# profile g.8275.1 clock-type T-BC
RP/0/RP0/CPU0:router(config-ptp-clock)# exit
```

clock

To enter Precision Time Protocol (PTP) clock configuration mode and run PTP clock configuration command, use the **clock** command in PTP configuration mode.

clock

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global PTP configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example shows how to enter PTP clock configuration mode from global configuration mode.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# clock
RP/0/RP0/CPU0:router(config-ptp-clock)#
```

delay-request

To configure settings for the PTP delay request message, use the **delay-request** command in PTP profile configuration mode.

delay-request frequency *frequency*

Syntax Description

frequency *frequency*	Specifies multiple announce messages per second (2, 4, 8, 16, 32, 64, or 128). Frequency of 4 means that four messages are sent per second.

Command Default

The default is one second between messages.

Command Modes

PTP configuration mode

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example sets the delay request frequency in the PTP configuration profile to 16 seconds.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# profile p1
RP/0/RP0/CPU0:router(config-ptp-profile)# delay-request frequency 16
```

domain

To specify the domain number for the PTP clock, use the **domain** command in PTP clock configuration mode.

domain *number*

Syntax Description

number	Specifies the domain number to use for this clock (0-255).

Command Default

Default is 0.

Command Modes

PTP clock configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example sets the domain to 24.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# clock
RP/0/RP0/CPU0:router(config-ptp-clock)# domain 24
```

log

To enable logging of changes to the best master clock for Precision Time Protocol (PTP), use the **log best-master-clock changes** command in PTP configuration mode.

log best-master-clock changes

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

PTP configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
logging	read, write

Example

The following example sets up PTP to log the best master clock changes.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# log best-master-clock changes
```

profile

To enter Precision Time Protocol (PTP) profile configuration mode and run PTP profile configuration commands, use the **profile** command in PTP configuration mode.

profile *name*

Syntax Description

profile *name*	Enters PTP profile configuration mode for the specified profile name.

Command Default

No default behavior or values.

Command Modes

PTP configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example shows how to configure the profile tp128.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# profile tp128
```

ptp

To enter Precision Time Protocol (PTP) configuration mode and run PTP configuration commands, use the **ptp** command in global configuration mode.

ptp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example shows how to enter PTP configuration mode from global configuration mode.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)#
```

sync

To configure settings for PTP sync messages, use the **sync** command in PTP profile configuration mode.

sync frequency *frequency*

Syntax Description

frequency *frequency*	Use to specify multiple sync messages per second (2, 4, 8, 16, 32, 64, or 128). Frequency of 4 means that four messages are sent per second.

Command Default

No default behavior or values.

Command Modes

PTP profile configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example sets the PTP sync timeout to 16 milliseconds.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# profile p1
RP/0/RP0/CPU0:router(config-ptp-profile)# sync frequency 2000
```

transport

To specify the PTP transport type, use the **transport** command in PTP profile configuration mode.

transport ethernet

Syntax Description

ethernet	Specifies that Ethernet is used as the transport type on the interface.

Command Default

No default behavior or values.

Command Modes

PTP profile configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Task ID

Task ID	Operations
ethernet-services	read, write

Example

The following example sets the transport type to be Ethernet.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# profile p1
RP/0/RP0/CPU0:router(config-ptp-profile)# transport ethernet
```

Zero Touch Provisioning (ZTP) Commands

This chapter describes the commands used to manually invoke Zero Touch Provisioning (ZTP).

ztp clean

To remove all ZTP logs and settings saved on disk, use the **ztp clean** command in EXEC mode.

ztp clean [debug] [verbose]

Syntax Description

debug	Run with additional logging to the console.
verbose	Run with logging to the console.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

If you wish to run ZTP as if from a clean boot, use the **ztp clean** command to remove all ZTP logs and settings. Use **commit replace** to reload, and then ZTP will run again as if from first boot.

No progress logs are shown by default, although there will be XR syslogs for important events. If you wish to see more logs, add **verbose** after the **ztp clean** command. If these logs are not enough, add **debug** before **verbose**.

Logs can be found in **disk0:/ztp/ztp.log**.

Example

The following example shows how to remove all ZTP files saved on the disk.

```
RP/0/RP0/CPU0:router# ztp clean verbose
Mon Oct 10 17:03:43.581 UTC
Remove all ZTP temporary files and logs? [confirm] [y/n] :y
All ZTP files have been removed.
If you now wish ZTP to run again from boot, do 'conf t/commit replace' followed by reload.
```

ztp initiate

To invoke a new ZTP DHCP session, use the **ztp initiate** command in EXEC mode.

ztp initiate {apply *configuration* **| [debug] [verbose]}**

Syntax Description

apply *configuration*	XR configuration commands to apply
debug	Run with additional logging to the console
verbose	Run with logging to the console

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

Use the **ztp initiate** command to forceably inititate the ZTP, ignoring username configuration. **ztp initiate** allows the execution of a script even when the system has already been configured. This command is useful for testing ZTP without forcing a reload. This command is particularly useful to test scripts or if some manual operations are required before provisioning the router.

No progress logs are shown by default, although there will be XR syslogs for important events. If you wish to see more logs, add **verbose** after the **ztp initiate** command. If these logs are not enough, add **debug** before **verbose**.

Logs can be found in **disk0:/ztp/ztp.log**.

Example

The following example shows how to bring up the interface manually.

```
RP/0/RP0/CPU0:router# ztp initiate debug verbose
Invoke ZTP? (this may change your configuration) [confirm] [y/n]:
```

ztp terminate

To terminate all the existing ZTP processes, use the **ztp terminate** command in EXEC mode.

ztp terminate [debug] [verbose] [noprompt]

Syntax Description

debug	Run with additional logging to the console.
verbose	Run with logging to the console.
noprompt	Run without prompting.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

If you want to terminate an already running ZTP process, use the **ztp terminate** command. Be careful to use the **ztp terminate** command because unproperly usage of this command may leave your system in a partially configured state.

No progress logs are shown by default, although there will be XR syslogs for important events. If you wish to see more logs, add **verbose** after the **ztp terminate** command. If these logs are not enough, add **debug** before **verbose**.

Logs can be found in **disk0:/ztp/ztp.log**.

Example

The following example shows how to terminate the ZTP sessions in progress.

```
RP/0/RP0/CPU0:router# ztp terminate verbose
Mon Oct 10 16:52:38.507 UTC
Terminate ZTP? (this may leave your system in a partially configured state) [confirm] [y/n]:y
ZTP terminated
```

Authentication, Authorization, and Accounting Commands

This module describes the commands used to configure authentication, authorization, and accounting (AAA) services.

secret

To configure an encrypted or clear-text password for the user, use the **secret** command in username configuration mode or line template configuration mode. To remove this configuration, use the **no** form of this command.

secret [*0* [**enc-type** *enc-type-value*] **|5|8|9|10**] *secret-login*

no secret

Syntax Description

0	(Optional) Specifies that an unencrypted (clear-text) password follows. The password will be encrypted for storage in the configuration using an MD5 encryption algorithm. Otherwise, the password is not encrypted.
5	Specifies that an encrypted MD5 password (secret) follows.
8	(Optional) Specifies that SHA256-encrypted password follows.
9	(Optional) Specifies that scrypt-encrypted password follows.
10	(Optional) Specifies that SHA512-encrypted password follows.
secret-login	Text string in alphanumeric characters that is stored as the MD5-encrypted password entered by the user in association with the user's login ID. **Note** The characters entered must conform to MD5 encryption standards.
enc-type	(Optional) Configures the encryption type for a password entered in clear text.
enc-type-value	Specifies the encryption type to be used.

Command Default

No password is specified.

Command Modes

Username configuration

Line template configuration

Command History

Release	Modification
6.5.33	This command was introduced.

Usage Guidelines

Secrets are one-way encrypted and should be used for login activities that do not require a decryptable secret.

Task ID

Task ID	Operation
aaa	read, write

Example

The following example shows how to establish the clear-text secret “lab” for the user user2 :

```
RP/0/RP0/CPU0:ios(config)#username cisco
RP/0/RP0/CPU0:ios(config-un)#secret ?
RP/0/RP0/CPU0:ios(config-un)#secret 9
$9$q8j4v/mf1SOg5v$nGAhRkf0ek3wSYjDG/VKhwp2znPaWusuZtkx9Z1sM
```

policy

To configure a policy that is common for user password as well as secret, use the **policy** command in username configuration mode. To remove this configuration, use the **no** form of this command.

policy *policy-name*

Syntax Description

policy-name	Specifies the name of the policy that is common for user password as well as secret.

Command Default

None

Command Modes

username

Command History

Release	Modification
6.5.33	This command was introduced.

Usage Guidelines

For detailed usage guidelines for this command, see the section of *AAA Password Secuirity Policies* chapter of *Configure Authentication for Cisco NCS 4000*

Task ID

Task ID	Operation
aaa	read, write

Example

This example shows how to configure a password policy that applies to both the password and the secret of the user.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#username test_1
RP/0/RP0/CPU0:router(config-un)#policy test-policy1
RP/0/RP0/CPU0:router(config-un)#secret 10
$6$dmwuW0Ajicf98W0.$y/vzynWF1/OcGxwBwHs79VAy5ZZLhoHd7TicR4mOo8IIVriYCGAKW0A.w1JvTPO7IbZry.DxHrE3SN2BBzBJe0
RP/0/RP0/CPU0:router(config-un)#commit
```

username

To configure a new user with a username, establish a password, associate a password policy with the user, grant permissions for the user, and to enter username configuration mode, use the **username** command in XR Config mode or System Admin Config mode. To delete a user from the database, use the **no**form of this command.

username *name*
no username *name*

Syntax Description

username	Name of the user. The name argument can be only one word. Spaces and quotation marks are not allowed.

Command Default

No usernames are defined in the system.

Command Modes

Command History

Release	Modification
6.5.33	This command was introduced.

Usage Guidelines

Use the **username** command to identify the user and enter username configuration mode.

Task ID

Task ID	Operation
aaa	read, write

Example

The following example shows the commands available after executing the **username** command:

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#username user1
```

Link Layer Discovery Protocol (LLDP) Command Reference

This chapter describes the commands to configure LLDP.

lldp

To enable the Link Layer Discovery Protocol (LLDP) globally for both transmit and receive operation on the system, use the **lldp** command in XR Config mode. To disable LLDP, use the **no** form of this command.

lldp

no lldp

Syntax Description

lldp	Enables or disables LLDP globally for both transmit and receive operation on the system.

Command Default

None

Command Modes

Config mode

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to enable LLDP globally for both transmit and receive operation on a system.:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# lldp
```

lldp holdtime

Use the **lldp holdtime** command to specify the hold time for the receiving device to hold the information from an LLDP packet before aging and removing it. To return to the default, use the **no** form of this command.

lldp holdtime *seconds*

no lldp holdtime

Syntax Description

seconds	Specify the time in seconds to hold the packet information. Default value: 120

Command Default

None

Command Modes

Config mode

Usage Guidelines

None

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to specify the hold time:

```
RP/0/RP0:hostname(config)# lldp holdtime 60
```

Topic 2.1

lldp reinit

Use the **lldp reinit** command to specify the time to delay the initialization of LLDP on an interface. To return to the default, use the **no** form of this command.

lldp reinit *seconds*

no lldp reinit

Syntax Description

seconds	Specify the time in seconds for which LLDP should delay initialization. Default value: 2

Command Default

None

Command Modes

Config mode

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to specify the time to delay the initialization of LLDP on an interface:

```
RP/0/RP0:hostname(config)# lldp reinit 4
```

lldp timer

Use the **lldp timer** command to specify the interval at which the device sends LLDP packets to neighboring devices. To return to the default, use the **no** form of this command.

lldp timer *seconds*

no lldp timer

Syntax Description

seconds	Specify the interval in seconds. Default value: 30

Command Default

None

Command Modes

Config mode

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to LLDP time interval:

```
RP/0/RP0:hostname(config)# lldp timer 60
```

lldp tlv-select

Use the **lldp tlv-select** command to disable transmission of the selected Type Length Value (TLV) in LLDP packets. To return to the default, use the **no** form of this command.

lldp tlv-select *tlv-name* **disable**

no lldp tlv-select

Syntax Description

tlv-name	Name of the TLV to be suppressed from LLDP packets. Valid TLV values: • management-address • port-description • system-capabilities • system-description • system-name
disable	Disables the specified TLV.

Command Default

None

Command Modes

Config mode

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to disable transmission of the *system-capabilities* TLV from LLDP packets:

```
RP/0/RSP0/CPU0:router(config)# lldp tlv-select system-capabilities disable
```

receive disable

Use the **receive disable** command to disable the reception of LLDP packets on an interface. To return to the default, use the **no** form of this command.

receive disable

no receive disable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

LLDP configuration

Usage Guidelines

None

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to disable LLDP receive operations on an interface:

```
RP/0/RP0:hostname(config-if)# lldp
RP/0/RP0:hostname(config-if-lldp)# receive disable
```

transmit disable

Use the **transmit disable** command to disable the transmission of LLDP packets from an interface. To return to the default, use the **no** form of this command.

transmit disable

no transmit disable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

LLDP configuration

Usage Guidelines

None

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to disable LLDP receive operations on an interface:

```
RP/0/RP0:hostname(config-if)# lldp
RP/0/RP0:hostname(config-if-lldp)# transmit disable
```

show lldp

Use the **show lldp** command to display the global LLDP configuration status and the operational characteristics of the system.

show lldp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

LLDP configuration

Command History

Release	Modification
Release 6.5.33	This command was introduced.

Usage Guidelines

The **show lldp** command displays the LLDP status and operational characteristics when LLDP is enabled globally on the system using the **lldp** command. The settings for the following commands are displayed:

- **lldp timer**
- **lldp holdtime**
- **lldp reinit**

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to display the default LLDP operational characteristics when LLDP is enabled globally on the system:

```
RP/0/RP0:hostname# show lldp
Wed Dec 13 06:16:45.510 DST
    Global LLDP information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

show lldp interface

Use the **show lldp interface** display LLDP configuration and status information on an interface.

show lldp interface *type interface-path-id*

Syntax Description

type	Specify the interface type.
interface-path-id	Specify the physical interface or virtual interface ID in the rack/slot/module notation. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.

Command Default

LLDP configuration and status information for all interfaces is displayed.

Command Modes

EXEC mode

Task ID

Task ID	Operation
ethernet-services	read

Example

The following example shows sample output for the **show lldp interface** command for the Ten Gigabit Ethernet interface at 0/1/0/7:

```
RP/0/RP0:hostname# show lldp interface TenGigE 0/1/0/7
Wed Dec 13 13:22:30.501 DST
    TenGigE0/1/0/7:
    Tx: enabled
    Rx: enabled
    Tx state: IDLE
    Rx state: WAIT FOR FRAME
```

Table 91: show lldp interface Field Descriptions

Field	Description
Tx:	Configuration status of the interface to transmit LLDP advertisements.
Rx:	Configuration status of the interface to receive LLDP advertisements.
Tx state:	Status of the LLDP transmit process on the interface.
Rx state:	Status of the LLDP receive process on the interface.

show lldp neighbors

Use the **show lldp neighbors** command to display the basic details of the neighbor devices.

show lldp neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

Basic device information for LLDP neighbors is displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.5.33	This command was introduced.

Task ID

Task ID	Operation
ethernet-services	read

Example

The following example shows sample output for the **show lldp neighbors** command:

```
RP/0/RP0:ios#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

    Device ID      Local Intf         Hold-time     Capability         Port ID
    R1         TenGigECtrlr0/5/0/4/1     150            R        TenGigECtrlr0/5/0/4/1
    Total entries displayed: 1
```

Table 92: show lldp neighbor Field Descriptions

Field	Description
Device ID	Name of the neighbor device.
Local Interface	Displays the interface on which the LLDP packet is received.
Hold Time	Time (in seconds) that the local device will hold the LLDP advertisement from a sending device before discarding it.
Capability	Name of the system capability advertised by the neighbor. Capabilities are represented in a bitmap that defines the system's primary functions.

Field	Description
Port ID	Displays the Port identifier that identifies the port component of the endpoint identifier associated with the transmitting LLDP agent.

show lldp neighbors detail

Use the **show lldp neighbors detail** command to display the neighbor devices details such as system description, name, and capabilities.

show lldp neighbors detail

Syntax Description

This command has no arguments or keywords.

Command Default

Detailed device information for LLDP neighbors is displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.5.33	This command was introduced.

Task ID

Task ID	Operation
ethernet-services	read

Example

The following example shows sample output for the **show lldp neighbors detail** command:

```
RP/0/RP0:ios#show lldp neighbors detail
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
    ------------------------------------------------
    Local Interface: TenGigECtrlr0/5/0/4/1
    Chassis id: 22 33
    Port id:
    Port Description - not advertised
    System Name - not advertised
    System Description - not advertised
    Time remaining: 16 seconds
    Hold Time: 17 seconds
    System Capabilities: N/A
    Enabled Capabilities: N/A
    Management Addresses - not advertised
    Peer MAC Address: 10:02:03:04:05:06
    Total entries displayed: 1
```

Table 93: show lldp neighbor details Field Descriptions

Field	Description
Local Interface	Displays the interface on which the LLDP packet is received.

Field	Description
Chassis id	Displays the chassis component of the endpoint identifier associated with the transmitting LLDP agent.
Port id	Displays the port ID that identifies the port component of the endpoint identifier associated with the transmitting LLDP agent.
Port Description	Displays the description of the port associated with the interface on which the LLDP agent is transmitting.
System Name	Displays the system's administratively assigned name.
System Description	Displays the description of the network entity.
Time remaining	Displays the remaining time.
Hold Time	Displays the time or duration in seconds that an LLDP device maintains the neighbor information before discarding.
System Capabilities	Displays a bit-map of the capabilities that define the primary functions of the system. A system may advertise more than one capability.
Enabled Capabilities	Indicates whether the corresponding system capability is enabled on the neighbor.
Management Addresses	Displays a network address of the remote device.
Peer MAC Address	Displays the source MAC address in the received LLDP packet.

Daisy Chain Network Command Reference

This chapter describes the commands to configure Daisy Chain Network.

bridge-port routed-interface

Use the **bridge-port routed-interface** command to bridge two ports. For example, when connecting multiple NCS 4000 devices in a Daisy Chain topology, use this command to bridge the EMS and Craft ports so that the traffic on EMS port is routed towards the Craft port.

bridge-port routed-interface *type interface-path-id*

Syntax Description

type	Specify the Management Ethernet interface.
interface-path-id	Specify the physical or virtual interface.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 6.5.33	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
ethernet-services	read, write

Example

The following example shows how to bridge the Craft and EMS ports:

```
RP/0/RP0:Node-41(config)#interface MgmtEth0/RP0/EMS/0
RP/0/RP0:Node-41(config-if)#no shutdown
RP/0/RP0:Node-41(config-if)#ipv4 address 192.168.02.01/24
RP/0/RP0:Node-41(config)#interface MgmtEth0/RP0/CRAFT/0
RP/0/RP0:Node-41(config-if)#bridge-port routed-interface MgmtEth0/RP0/EMS/0
RP/0/RP0:Node-41(config-if)#no shutdown
```

Table 94: Related Commands

Command	Description
interface (OSPF), on page 273	Use this command in area configuration mode to define the interfaces on which the Open Shortest Path First (OSPF) protocol runs.
shutdown (IS-IS)	Use this command to enable the Intermediate System-to-Intermediate System (IS-IS) protocol on a particular interface.
ipv4 address odu	Use this command to configure IP address for GCC on an ODUk controller.

INDEX

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W