Configuration Guide for Cisco NCS 4000 Series

First Published: 2015-05-25

Last Modified: 2024-07-05

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

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 commands available to configure and maintain the Cisco NCS 4000 Series.

Audience

The Cisco IOS XR documentation set is intended primarily for users who configure and maintain Cisco networking devices (such as routers and 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, configuration options, in the OTN IOS XR for Cisco NCS 4000 Series Router.

Related Documentation

Use this guide in conjunction with the following referenced publications:

- *Command Reference for Cisco NCS 4000 Series*
- *Troubleshooting Guide for Cisco NCS 4000 Series*
- *Cisco IOS XR System Error Message Reference Guide*
- *TL1 Guide for Cisco NCS 4000 Series*
- *Hardware Installation Guide for Cisco NCS 4000 Series*
- *Regulatory Compliance and Safety Information for the Cisco NCS 4000 Series*

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier font`	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:

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

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

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

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

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

IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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

BEWAAR DEZE INSTRUCTIES

Varoitus

TÄRKEITÄ TURVALLISUUSOHJEITA

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

SÄILYTÄ NÄMÄ OHJEET

Attention

IMPORTANTES INFORMATIONS DE SÉCURITÉ

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

CONSERVEZ CES INFORMATIONS

Warnung

WICHTIGE SICHERHEITSHINWEISE

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

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza

IMPORTANTI ISTRUZIONI SULLA SICUREZZA

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

CONSERVARE QUESTE ISTRUZIONI

Advarsel

VIKTIGE SIKKERHETSINSTRUKSJONER

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

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso

INSTRUÇÕES IMPORTANTES DE SEGURANÇA

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

GUARDE ESTAS INSTRUÇÕES

¡Advertencia!

INSTRUCCIONES IMPORTANTES DE SEGURIDAD

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

GUARDE ESTAS INSTRUCCIONES

Varning!

VIKTIGA SÄKERHETSANVISNINGAR

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

SPARA DESSA ANVISNINGAR

Figyelem

FONTOS BIZTONSÁGI ELOÍRÁSOK

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение

ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告

重要的安全性说明

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

请保存这些安全性说明

警告

安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

주의

중요 안전 지침

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

이 지시 사항을 보관하십시오.

Aviso

INSTRUÇÕES IMPORTANTES DE SEGURANÇA

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

GUARDE ESTAS INSTRUÇÕES

Advarsel

VIGTIGE SIKKERHEDSANVISNINGER

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

GEM DISSE ANVISNINGER

تحذير

إرشادات الأمان الهامة

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

قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

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

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

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

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

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

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

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

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

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

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

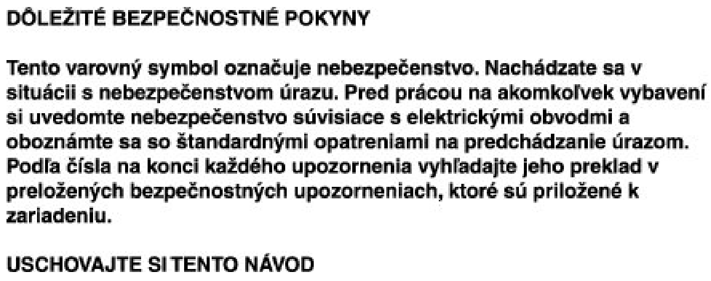
Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

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

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie



DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

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

USCHOVAJTE SI TENTO NÁVOD

PART I

Configurations Using CTC

CHAPTER 1

Configure Authentication

This chapter describes the procedures to create users and configure authentication.

Understand Authentication

Authentication is a way of identifying a user before permitting access to the network and network services. When Authentication is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it. Cisco NCS 4000 series uses the RADIUS/TACACS+ server for authenticating remote users.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS is a client/server protocol that runs in the application layer that uses User Datagram Protocol (UDP) for transport.

The RADIUS server process runs in background on a UNIX or Microsoft Windows server and client would be the Cisco network element (NE). RADIUS clients run on Cisco routers and sends the authentication requests to a central RADIUS server that contains all the user authentication and network service access information.

TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is a new protocol developed by Cisco and released as an open standard. TACACS+ uses TCP for transport. TACACS+ protocol is a security application that provides centralized validation of users attempting to gain access to a network element. Since, TCP is connection oriented protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout and others, as it rides on UDP that is connectionless. RADIUS encrypts only the user password as it travels from the RADIUS client to RADIUS server. All other information, for example, username, authorization, and accounting are transmitted in clear text. Therefore, it is vulnerable to various types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.

Create a Local User on a Single Node Using CTC

Purpose	This procedure enables you to create a local user on a single or multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

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

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

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

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

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

  The minimum password length for CTC is six and maximum of 20 characters. . The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%,~,!,@,$,+,^,&,*,(),<>,{},[],-._,=) characters, where at least two characters are not alphabetic and at least one character is a special character; or the password can contain any character. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: **RETRIEVE**, **MAINTENANCE**, **PROVISIONING**, or **SUPERUSER**.

- Retrieve—Users can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance—Users can access only the maintenance options.
- Provisioning—Users can access the provisioning and maintenance options.
- Superusers—Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.

Step 4 Click **OK**.

Stop. You have completed this procedure.

Viewing and Retrieving Active Logins

Purpose	This procedure enables you to view active CTC logins, retrieve the last activity time.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	All users

Procedure

Step 1 In node view or network view, click the **Provisioning** > **Security** > **Active Logins** tabs. The Active Logins tab displays the following information:

- Node
- User
- Source IP address
- Session Type (EMS, TL1, FTP, Telnet, or SSH)
- Login time
- Last activity time

Note Active Login tab always display the two telnet sessions for a single CTC session, open by a user using a single IP address.

Step 2 Click **Retrieve Last Activity Time** to display the most recent activity date and time for users in the Last Activity Time field.

Stop. You have completed this procedure.

Configure Authentication Server Order

Purpose	This procedure enables you to configure the order of the servers for DUO Two-Factor authentication.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Important Before you configure the server authentication order, log in to the node using the local username and password.

Procedure

Step 1 In node view or network view, click the **Provisioning** > **Security** > **Radius / Tacacs+** tabs.

The Radius / Tacacs+ tab displays the Authentication Mode and Server in Order of Authentication panes.

Step 2 In the Authentication Mode pane, choose: **Radius**, **Tacacs+**, or **Local**.

(Optional) Check the **Node As Final Authentication When No Server Is Found** check box.

Step 3 In the **Server in Order of Authentication** pane, click **Add** and enter the following.

- Server Type—Displays the selected server type.
- Node Address—IPv4 address of the current node
- Shared Secret—Secret key shared between the client node and the cloud server
- Encrypted—Encrypts and decrypts the authentication data.
- Authentication Port—Authentication port value of the selected server type
- Accounting Port—Accounting port value of the selected server type

Alternatively, you can add the server profile by executing the following CLI command:

```
radius-server host 10.xx.xx.xxx auth-port 1812 acct-port 1813 key ravk@1234
```

Note If more than one server profile is created, the profile at the top is used for authenticating first. Use the following buttons to change the order of the authentication servers:

- Delete—Deletes the created server type.
- Move Up—Moves the server profile up the order.
- Move Down—Moves the server profile down the order.

Step 4 Click **Apply**.

What to do next

Log in using the new username and password stored in the cloud server from the next session.

CHAPTER 2

Configure the NCS4K-2H-W Card

This chapter explains the NCS4K-2H-W card and its key features. This chapter also provides the CTC procedures to configure the card.

NCS4K-2H-W Card

The DWDM cards is a tunable DWDM trunk card, which simplifies the integration and transport of two 100 Gigabit Ethernet or OTU-4 signals into enterprises or service provider networks. The card is ITU-T G.709 compliant and supports 96 wavelengths, spaced at 50-GHz over the entire C band. The card is supported on Cisco NCS 4000 series.

The card has two pluggable client interfaces that can be used to provide transponder capabilities. The client port supports pluggable interface that is compliant with 100G-BASESR10 LAN PHY or OTU4 and 100G-BaseLR-4 or OTU4 interfaces. The trunk port supports only the OTU4 interface. The trunk ports support Baud rate between 27.952 Gbaud and 31.241 Gbaud, depending on FEC selection and G.709v3 OTU4 digital wrapper. The card can be installed in any line card slot in the Cisco NCS 4000 chassis.

Key Features of NCS4K-2H-W Card

The NCS4K-2H-W card supports the following key features:

- Operating Modes—The card can be configured in different operating modes: The cards can be equipped with pluggables for client and trunk options, and offer a large variety of configurations.

- Transponder—This mode is enabled by default. The card acts as a transponder in this mode. Each client is mapped to one of the two 100 Gigabit Ethernet NCS4k-2H-W interfaces providing up to thirty-two 100 Gigabit NCS4k-2H-W transponders. In transponder mode, the allowed port pairs are 0-2 and 1-3.
- Regeneration—The two 100 Gigabit NCS4k-2H-W interfaces are connected back-to-back in the card to provide 3R regeneration of 100 Gigabit NCS4k-2H-W signals. In regeneration mode, an IP-over-NCS4k-2H-W configuration can be enabled to support proactive protection messaging between IP-over-NCS4k-2H-W router interfaces. If failure occurs on one side of the regenerator, ODUk Alarm Indication Signal (ODUk-AIS) is generated and propagated on the other side, while an OTUk Backwards Defect Indicator (OTUk-BDI) is sent back on the same side as defined by the ITU G.709 standard. In Regeneration mode, the allowed port pair is 2-3.

When you configure the card in different operating modes, ensure NCS4k-2H-W that the following tasks are completed:

- Depending on the card mode selected, the supported payload for that particular card mode must be provisioned on the PPMs.
- The payloads can be provisioned after configuring the operating mode on the card.

The following table describes how each mode can be configured, the supported payloads, and the valid port pair for a specific operating mode.

Operating Mode	Port Number	Peer Card (connected through backplane)	Port Mode	Mapping	Framing Type	Supported Client Payloads
Transponder	0 and 1	—	OTN	—	OPU4	OTU4
Transponder	0 and 1	—	Ethernet	GMP	OPU4	100GE over ODU4
Transponder and Regeneration	2 and 3	NCS4K-20T-O-S, NCS4K-2H-O-K	OTN	—	OPU4	OTU4

See the Provision an Operating Mode Using CTC, on page 10 procedure to provision the operating mode.

- Forward Error Correction (FEC)—The trunk ports support three different FEC coding options:
  - GFEC: Standard G.975 Reed-Solomon algorithm with 7-percent overhead.
  - Ultra FEC (UFEC): Standard G.975.1 (Sub-clause I.7) with 20-percent overhead.
  - High-gain FEC (HG-FEC): HG-EFEC with 7-percent and 20-percent overhead provides better performance than standard G.975.1 7-percent overhead enhanced FEC. This EFEC is suitable for applications where 100 Gigabit wavelengths pass through a large number of ROADM nodes with limited performance.
- Generalized Multiprotocol Label Switching—The Generalized Multiprotocol Label Switching (GMPLS) OCH Trail circuit can be created on the NCS4K-2H-W card. The OCH Trail circuit can created between source and destination NCS 4000 series nodes that are connected to the ONS 15454 nodes. The OCH Trail circuit creates an optical connection from the source trunk port to the destination trunk port. The

interface on the NCS 4000 node is the UNI-C interface and the interface on the ONS 15454 node is the UNI-N interface.

- Performance Monitoring—The 100-Gbps NCS4k-2H-W trunk provides support for both transparent and non-transparent signal transport performance monitoring. The Digital Wrapper channel is monitored according to G.709 (OTN) and G.8021 standards. Performance Monitoring of optical parameters on the client and NCS4k-2H-W line interface include Loss Of Signal (LOS), Laser Bias Current, Transmit Optical Power, and Receive Optical Power. The calculation and accumulation of the performance monitoring data are supported in 15-minute and 24-hour intervals as per G.7710. The system parameters measured at the wavelength level like Mean PMD, accumulated Chromatic Dispersion, or Received OSNR are also included in the set of performance monitoring parameters. These can greatly simplify troubleshooting operations and enhance the set of data which can be collected directly from the equipment.

For more information on the NCS4K-2H-W card, see the data sheet.

Automatic Power Consumption

CTC dynamically displays the power consumption of each card inserted in the chassis. CTC also dynamically displays the power budget for the entire system and for each slot. The maximum power is always allocated for each route processor, fabric card, and fan tray. A minimum power budget is allocated for each line card. The minimum power budget for each line card is the maximum of the minimum power allocated to any type of line card. For example, if the NCS4K-2H-O-K card has 35 W and NCS4K-2H-W card has 50 W, then minimum power budget allocated for each line card slot is 50 W. When a line card is inserted or removed, the minimum power budget for each line card is dynamically re-calculated and displayed in CTC.

When a line card is inserted, the maximum power budget is allocated if enough power is available; otherwise, the card is shut down and a major alarm is raised in the Alarms tab. A minor alarm is raised when the power allocation is more than the available power.

Monitor Environmental Parameters Using CTC

Purpose	This procedure monitors the environmental parameters of the NCS4K-2H-W card such as temperature, voltage, and power.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to monitor the environmental parameters. The card view appears.

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

Step 3 Click **Temperature** sub-tab to display the input temperature of the card.

- Module Sensor—Displays the module sensor name of the card.
- Value (Celsius)—Displays the module sensor values (in Celsius) of the card.

Step 4 Click **Voltage** sub-tab to display the input voltage of the card.

- Module Sensor—Displays the module sensor name of the card.
- Value (MilliVolts)—Displays the module sensor values (in MilliVolts) of the card.

Step 5 Click **Power Monitor** sub-tab to dynamically display the power consumption of the card.

- Module Sensor—Displays the module sensor name of the card.
- Value (MilliAmperes)—Displays the module sensor values (in MilliAmperes) of the card.

Stop. You have completed this procedure.

Provision an Operating Mode Using CTC

Purpose	This procedure enables you to provision an operating mode on the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision an operating mode. The card view appears.

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

Step 3 In the **Card Mode** area, choose the required operating mode: **TXP** or **Regeneration**.

The **Backplane** mode is not supported.

Step 4 Choose **TXP** to provision the card in Transponder (TXP) mode and click **Apply**.

Step 5 If you want to provision the card in Regeneration mode, follow these steps.

a) Choose **Regeneration**.

The regeneration is applicable only for NCS4K-2H-W.

b) Choose the port number from the Port1 drop-down list. The available option is 2 or 3.

c) Click **Apply**.

Stop. You have completed this procedure.

Administrative and Service States

Administrative State	Definition
IS	Puts the entity in service.
OOS,DSBLD	Removes the entity from service and disables it.
OOS,MT	Removes the entity from service for maintenance.

Service State	Definition
OOS-MA,DSBLD	The entity was manually removed from service and does not provide its provisioned functions. All the services are disrupted and unable to carry traffic.
OOS-MA,MT	The entity has been manually removed from service for a maintenance activity but still performs its provisioned functions.
OOS-AUMA,FLT&MT	The entity is not operational because of an autonomous event and has also been manually removed from service for a maintenance activity.
OOS-MA,LPBK&MT	The entity has been manually removed from service for a maintenance activity but still performs its provisioned functions. A loopback is present on the resource.
OOS-AUMA, FLT & LPBK & amp; MT	The entity is unlocked with loopback configured. However, the service is not operational due to some failure. All the defects are raised and cleared but the end user is not notified.
OOS-AU,AINS	The entity is not operational because of an autonomous event. The entity is delayed before moving to the IS-NR state.
OOS-AU,AINS&FLT	The entity is unlocked. However, the service is not operational due to some failure. All the defects are raised and cleared but the end user is not notified. When all the defects are cleared and the resource returns operational, the AINS window is restarted.
IS-NR	The entity is fully operational and will perform as provisioned.
OOS-AU,FLT	The entity is unlocked and not operational due to a failure. This happens when the secondary state is normal and there are defects.

Provision the NCS-4K-2H-W Ports Using CTC

Purpose	This procedure provisions the ports on the NCS-4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following tasks as needed:

- Provision NCS4K-2H-W Optics Controllers Using CTC, on page 12
- Provision NCS4K-2H-W 100GE Payload Using CTC , on page 14
- Provision NCS4K-2H-W OTU4 Payload Using CTC, on page 15
- Provision NCS4K-2H-W ODU4 Using CTC, on page 16
- Provision NCS4K-2H-W TCM Using CTC, on page 17

Stop. You have completed this procedure.

Provision NCS4K-2H-W Optics Controllers Using CTC

Purpose	This procedure enables you to provision the optics controllers on the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the optics controllers. The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > **Optics** tabs.

Step 3 Modify any of the settings described in the following table as needed.

Parameter	Description
Controller	Displays type and address of the controllers in the Rack/Slot/Instance/Port format.
Admin State	Sets the administrative state of the port. Choose an administrative state from the drop-down list to change the administrative state unless network conditions prevent the change. For more information, see Administrative and Service States, on page 11.
Service State	Displays the autonomously generated state that provides the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.
Optics Type	Displays the type of optics connected to this port. It can be Grey optics or NCS4k-2H-W optics.
Wavelength	If the optics type is Grey, the wavelength is 0.0 nm. If the optics type is NCS4k-2H-W, the wavelength can be one of the wavelengths chosen in the grid.
Laser Bias Current (%)	Displays the laser bias current in % between 0.0 and 100.0
Rx Power (dBm)	Displays the received power for the corresponding ports in dBm.
Tx Power (dBm)	Displays the transmitted power for the corresponding ports in dBm.
Laser State	Displays the state of the associated laser. The state can be On or Off.
VOATX Power	Sets the value for the desired TX power in the of range +0.2 / -19.0 dBm. The card sets the transmit VOA to match the required power. Applicable on trunk ports 2 and 3, in the OOS mode.
Optical Signal to Node	Displays the current value of received OSNR (Optical Signal to Noise Ratio) at the receiver port (only on trunk 2 and 3).
Polarization Dependency	Displays the loss that depends on the wave polarization in the fiber transmission.
Polarization Changes	Displays the rate of optical wave polarization changes in the fiber transmission.
Phase Noise	Displays the noise on the phase of the optical signal received on the fiber.
CD	Displays the Chromatic Dispersion of the received signal.
Different	Displays the variation of propagation delay in the fiber transmission.
Enable PM	Select the check-box to enable performance monitoring.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure.

Provision NCS4K-2H-W 100GE Payload Using CTC

Purpose	This procedure enables you to provision the client ports with 100GE payload on the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the 100GE Payload. The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > **Optics** tabs to provision 100GE payload on a client port (port 0 or port 1).

Step 3 Select a client port and choose OOS,DSBLD from the Admin State drop-down list and click **Apply**.

Step 4 Click the **Provisioning** > **Port Modules** tabs.

Step 5 Change Port Mode to Ethernet, Framing Type to OPU4, and Mapping to Gmp.

Step 6 Click the **Provisioning** > **Controllers** > **Ethernet** tabs to modify any of the settings as described in the following table.

Parameter	Description
Client Port	Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
Admin State	Sets the administrative state of the port. Choose an administrative state from the drop-down list to change the administrative state unless network conditions prevent the change. For more information, see Administrative and Service States, on page 11.
Service State	Displays the autonomously generated state that provides the overall condition of the port.
Operational State	Displays the state of link. The values are Up or Down.
LED State	Displays the state of LED. The values are On or Off.

Parameter	Description
Autonegotiation	Enable or disable autonegotiation by selecting the check-box. Autonegotiation negotiates flow control, duplex mode and remote fault information. Enable or disable link negotiation on both the ends of the link.
Speed	Displays the speed at which Ethernet port is operating. The available value is HundredGbps and cannot be modified.
Duplex	Enable or disable duplex mode by selecting the check-box. Enabling duplex means , both the ends of the communication channel can send and receive signals at the same time.
Flow Control	Displays the negotiated flow control mode. The available value is ingress when configured.

Step 7 Click **Apply**.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W OTU4 Payload Using CTC

Purpose	This procedure enables you to provision the client and trunk ports with OTU4 payload on the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the OTU4 payload. The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > **Optics** tabs to provision the OTU4 payload on a client or trunk port (ports 0, 1, 2, or 3).

Step 3 Select a client or trunk port and choose OOS,DSBLD from the Admin State drop-down list and click **Apply**.

Step 4 Click the **Provisioning** > **Port Modules** tabs.

Step 5 Change Port Mode to OTN and Framing Type to OPU4.

Step 6 Click the **Provisioning** > **Controllers** > **OTU** tabs to modify any of the settings as described in the following table.

Parameter	Description
Controller	Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
Admin State	Sets the administrative state of the port. Choose an administrative state from the drop-down list to change the administrative state unless network conditions prevent the change. For more information, see Administrative and Service States, on page 11.
FEC	Sets the mode of forward error correction. The available values are Standard, EnhancedHG7, and EnhancedHG20 for trunk ports (ports 2 and 3); the values are Standard and None for client ports (ports 0 and 1).
GCC0	Enables the general communication channel.
Service State	Displays the autonomously generated state that provides the overall condition of the port. For more information, see Administrative and Service States, on page 11.
Enable PM	Enables performance monitoring.

Step 7 Click **Apply**.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W ODU4 Using CTC

Purpose	This procedure enables you to provision ODU4 on the NCS4K-2H-W card. This procedure applies only to the 0, 1, 2, or 3 ports where OTU4 payload has been provisioned.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision or retrieve the ODU4 parameters. The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > **ODU** tabs.

Step 3 Modify any of the settings described in the following table as needed.

Parameter	Description
Controller	Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
Admin State	Sets the administrative state of the port. Choose an administrative state from the drop-down list to change the administrative state unless network conditions prevent the change. For more information, see Administrative and Service States, on page 11.
Service State	Displays the autonomously generated state that provides the overall condition of the port.
Resource State	Displays the state of resources that are connected.
GCC1	Enables the general communication channel.
Payload Type	Sets the payload type of the selected port.
Flex Type	Displays the flex type.
Flex BW	Displays the flex bandwidth.
Flex Tolerance	Displays the flex tolerance.
TPN	Sets the tributary port number (TPN) for the ODU4 port. The valid range of TPN is from 1 to 80.
TSG	Sets the tributary slot granularity (TSG) level on the ODU4 port. The valid values are 1.25G and 2.5G.
OWNER	Displays the number of owners.
No of TS	Sets the number of tributary slots (TS) for the ODU4 port.
Allocated TS	Displays the number of tributary slots that are assigned.
Enable PM	Enables performance monitoring for the corresponding port.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure.

Provision NCS4K-2H-W TCM Using CTC

Purpose	This procedure enables you to perform lockout.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the TCM. The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > **TCM** tabs.

Step 3 Select the **Controller Name**, for which you want to configure TCM, from the drop-down list.

Step 4 Modify any of the settings described in the TCM Threshold Table as needed.

Parameter	Description
TCM	Displays the TCMs ID from 1 to 6.
Enable TCM State	Enables the selected TCM.
Enable PM	Enables performance monitoring for the selected TCM.
TCM mode	Select the mode from the drop down menu. The available options are: • Transparent - TCM data is passed through without any change, fault management and performance monitoring parameters are not enabled. • Operational - fault management and performance monitoring parameters can be enabled. • NIM (Non-Intrusive Monitoring) - fault management and performance monitoring parameters are enabled but are read-only
LTC	Check the LTC box to enable this alarm. This check-box can be selected only when the TCM mode is Operational.
TIM	Check the TIM box to enable this alarm. This check-box can be selected only when the TCM mode is Operational.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure.

Provision the NCS-4K-2H-W Alarm Thresholds

Purpose	This procedure provisions the alarm thresholds of the NCS-4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following tasks as needed:

- Provision NCS4K-2H-W Optics Alarm Thresholds Using CTC, on page 19
- Provision NCS4K-2H-W OTU Alarm Thresholds Using CTC, on page 20
- Provision NCS4K-2H-W ODU Alarm Thresholds Using CTC, on page 21
- Provision NCS4K-2H-W TCM Alarm Thresholds Using CTC, on page 21

Stop. You have completed this procedure.

Provision NCS4K-2H-W Optics Alarm Thresholds Using CTC

Purpose	This procedure enables you to provision the optics alarm thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the optics alarm thresholds. The card view appears.

Step 2 Click the **Provisioning** > **Alarm Thresholds** > **Optics** tabs.

Step 3 Modify any of the settings described in the following table as needed.

Parameter	Description
Controller	Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
Rx Power High (dBm)	Sets the threshold for minimum receive power for the corresponding ports.
Rx Power Low (dBm)	Sets the threshold for maximum receive power for the corresponding ports.
LBC High (%)	Sets the LBC High. The high laser bias current (LBC-HIGH) threshold is the percentage of the normal laser bias current when the corresponding alarm is raised.
Tx Power High (dBm)	Sets the threshold for maximum transmit power for the corresponding ports.

Parameter	Description
Tx Power Low (dBm)	Sets the threshold for minimum transmit power for the corresponding ports.
CD Max (ps/nm)	Sets the threshold for maximum chromatic dispersion.
CD Min (ps/nm)	Sets the threshold for minimum chromatic dispersion.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure.

Provision NCS4K-2H-W OTU Alarm Thresholds Using CTC

Purpose	This procedure enables you to provision the OTU alarm thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the OTU alarm thresholds. The card view appears.

Step 2 Click the **Provisioning** > **Alarm Thresholds** > **OTU** tabs.

Step 3 Modify any of the settings described in the following table as needed.

Parameter	Description
Controller	Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
SF BER	Sets the signal fail bit error rate. The allowed values are 1E-5,1E-6,1E-7,1E-8, and 1E-9.
SD BER	Sets the signal degrade bit error rate. The allowed values are 1E-5,1E-6,1E-7,1E-8, and 1E-9.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure.

Provision NCS4K-2H-W ODU Alarm Thresholds Using CTC

Purpose	This procedure enables you to provision the ODU alarm thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the ODU alarm thresholds. The card view appears.

Step 2 Click the **Provisioning** > **Alarm Thresholds** > **ODU** tabs.

Step 3 Modify any of the settings described in the following table as needed.

Parameter	Description
Controller	Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
SF BER	Sets the signal fail bit error rate. The allowed values are 1E-5,1E-6,1E-7,1E-8, and 1E-9.
SD BER	Sets the signal degrade bit error rate. The allowed values are 1E-5,1E-6,1E-7,1E-8, and 1E-9.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure.

Provision NCS4K-2H-W TCM Alarm Thresholds Using CTC

Purpose	This procedure enables you to set SFSD values for TCM (Tandem Connection Monitoring) corresponding to an ODU alarm thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*

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

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to set SFSD values for TCM. The card view appears.

Step 2 Click the **Provisioning** > **Alarm Thresholds** > **TCM** tabs.

Step 3 Select the **Controller Name** from the drop-down list.

Step 4 Modify any of the settings described in the TCM Threshold table as needed.

Parameter	Description
TCM	Displays the TCMs (1-6) for the selected port.
SF BER	Sets the signal fail bit error rate. The allowed values are 1E-5,1E-6,1E-7,1E-8, and 1E-9.
SD BER	Sets the signal degrade bit error rate. The allowed values are 1E-5,1E-6,1E-7,1E-8, and 1E-9.

Note SF BER value can should not be greater than SD BER.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure.

Provision the NCS-4K-2H-W Card PM Parameter Thresholds

Purpose	This procedure provisions the PM parameter thresholds of the NCS-4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following tasks as needed:

- Provision NCS4K-2H-W Optics PM Thresholds, on page 23
- Provision NCS4K-2H-W Ethernet PM Thresholds, on page 25
- Provision NCS4K-2H-W HD FEC PM Thresholds, on page 27
- Provision NCS4K-2H-W OTU PM Thresholds, on page 29
- Provision NCS4K-2H-W ODU PM Thresholds, on page 33
- Provision NCS4K-2H-W TCM PM Thresholds, on page 36

Stop. You have completed this procedure.

Provision NCS4K-2H-W Optics PM Thresholds

Purpose	This procedure enables you to provision the optics PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the optics PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **Optics** tabs.

Step 3 Select the **TCA** (Threshold Crossing Alert) option from the drop-down menu.

The available options are -

- Customize - This option is not supported.
- Disable All - Select this option to disable TCA for all the parameters of a controller. The row colour is (turns) white to indicate that TCA is disabled.
- Enable All - Select this option to enable TCA for all the parameters of a controller. The row colour turns green to indicate that TCA is enabled.

Step 4 The displayed **Warning Thresholds** value is defined in the **Intervals** area.

Step 5 Select the or 1 Day radio-button to set the TCA interval. ClickModify the TCA settings for a controller port described in the following table as needed.

Parameter	Description
Controller	(Display only) Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
Laser Bias (high)	Sets the maximum laser bias.
Laser Bias (low)	Sets the minimum laser bias.
Input Power High (dBm)	Sets the high threshold for the input power TCA.
Input Power Low (dBm)	Sets the low threshold for the input power TCA .
Output Power High (dBm)	Sets the high threshold for the output power TCA.
Output Power Low (dBm)	Sets the low threshold for the output power TCA.
Chromatic Dispersion High (cd)	Sets the lchromatic dispersion (CD) value for the received signal.
Chromatic Dispersion Low (cd)	Sets the chromatic dispersion (CD) value for the received signal.
Second Order Polarization Mode Dispersion High (sopmd)	Displays the variation of the wave polarization in fiber transmission.
Second Order Polarization Mode Dispersion Low (sopmd)	Displays the variation of the wave polarization in fiber transmission.
Differential Group Delay Low	Displays the lower threshold value of the variation of propagation delay in the fiber transmission.
Differential Group Delay High	Displays the higher threshold value of the variation of propagation delay in the fiber transmission.
Optical Signal to Noise Ratio High	Sets the higher threshold value for the Optical Signal to Noise Ratio (OSNR). It is the ratio between the signal power level and the noise power level.
Polarization Dependent Loss High	Displays the loss that depends on the wave polarization in the fiber transmission .
Polarization Change Rate High	Displays the rate of optical wave polarization changes in the fiber transmission.
Phase Noise High	Displays the noise on the phase of the optical signal received on the fiber.

Step 6 Click **Apply**.

Step 7 In the Intervals area, select 15 Min or 1 Day, then click **Refresh** to view the updated threshold values.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W Ethernet PM Thresholds

Purpose	This procedure enables you to provision the Ethernet PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the optics Ethernet thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **Ethernet** tabs.

Step 3 Select the **TCA** (Threshold Crossing Alert) option from the drop-down menu.

The available options are -

- Customize - This option is not supported.
- Disable All - Select this option to disable TCA for all the parameters of a controller. The row colour is (turns) white to indicate that TCA is disabled.
- Enable All - Select this option to enable TCA for all the parameters of a controller. The row colour turns green to indicate that TCA is enabled.

Step 4 The displayed **Warning Thresholds** value is defined in the **Intervals** area.

Step 5 Modify any of the settings described in the following table as needed.

Parameter	**Description**
Controller	(Display only) Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.
rxTotalpkts	The number of received packets.
etherStatsOctets	The total number of octets of data received in the network.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including Frame Check Sequence (FCS) octets) and were otherwise well formed.

Parameter	Description
dot3StatsFcsErrors	The number of frames with frame check errors.
dot3StatsFrameTooLong	The number of packets that are at least 64 octets long, without a bad FCS, where the 802.3 length/type field did not match the computed DATA field length.
etherStatsjabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
etherStatsPkt64Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkt65to127Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkt128to255Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkt256to511Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkt512to1023Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkt1024to1518Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInMulticastPkts	The total number of multicast frames received error-free.
ifInBroadcastPkts	The number of packets delivered to a higher sub-layer and addressed to a broadcast address at this sub-layer.
ifOutUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutMulticastPkts	The number of multicast frames transmitted error-free.
ifOutBroadcastPkts	The number of packets requested by higher-level protocols and addressed to a broadcast address at this sub-layer, including those not transmitted.
TxTotalPkts	The number of transmitted packets.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
etherStatsPkts	The total number of received packets.

Parameter	Description
ifInOctets	Total number of octets received on the interface, including framing characters.
ifInErrors	Number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
etherstats (Broadcast / Multicast / Undersize packets)	Total number of packets received. • Broadcast - Total number of good packets received that were directed to the broadcast address. • Multicast - Total number of good packets received that were directed to the multicast address. • Undersize - Total number of good packets received that were less than 64 octets long.

Step 6 Click **Apply**.

Step 7 In the Intervals area, select 15 Min or 1 Day, then click **Refresh** to view the updated threshold values.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W HD FEC PM Thresholds

Purpose	This procedure enables you to provision the Hard Decision (HD) FEC PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the FEC PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **FEC** tabs.

Step 3 Select the **TCA** (Threshold Crossing Alert) option from the drop-down menu.

The available options are -

- Customize - This option is not supported.

- Disable All - Select this option to disable TCA for all the parameters of a controller. The row colour is (turns) white to indicate that TCA is disabled.
- Enable All - Select this option to enable TCA for all the parameters of a controller. The row colour turns green to indicate that TCA is enabled.

Step 4 The displayed **Warning Thresholds** value is defined in the **Intervals** area.

Step 5 Modify any of the settings described in the following table as needed.

Parameter	Description	Options
Controller	(Display only) Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.	—
EC-bits	The number of bit errors that are corrected by the system.	The valid range for the 15 min interval is from 0 to 9033621811200 (Default value is 903330). The valid range for the 1 day interval is from 0 to 867227693875200 (Default value is 8671968).
UC Words	The number of words that are not corrected by the system.	The valid range for the 15 min interval is from 0 to 4724697600 and 0 to 453570969600 for the 1 day interval.

Step 6 Click **Apply**.

Step 7 In the **Intervals** area, select 15 Min or 1 Day, then click **Refresh** to view the updated threshold values.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W SD FEC PM Thresholds

Purpose	This procedure enables you to provision the Soft Decision (SD) FEC PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the FEC PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **FEC** tabs.

Step 3 Select the **TCA** (Threshold Crossing Alert) option from the drop-down menu.

The available options are:

- Customize - This option is not supported.
- Disable All - Select this option to disable TCA for all the parameters of a controller. The row colour is (turns) white to indicate that TCA is disabled.
- Enable All - Select this option to enable TCA for all the parameters of a controller. The row colour turns green to indicate that TCA is enabled.

Step 4 The displayed **Warning Thresholds** value is defined in the **Intervals** area.

Step 5 Modify any of the settings described in the following table as needed.

Parameter	Description	Options
Controller	(Display only) Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.	—
EC-bits	The number of bit errors that are corrected by the system.	The valid range for the 15 min interval is from 0 to 9033621811200 (Default value is 903330). The valid range for the 1 day interval is from 0 to 867227693875200 (Default value is 8671968).
UC Words	The number of words that are not corrected by the system.	The valid range for the 15 min interval is from 0 to 4724697600 and 0 to 453570969600 for the 1 day interval.

Step 6 Click **Apply**.

Step 7 In the **Intervals** area, select 15 Min or 1 Day, then click **Refresh** to view the updated threshold values.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W OTU PM Thresholds

Purpose	This procedure enables you to provision the OTU PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the OTU PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **OTU** tabs.

Step 3 Select the **TCA** (Threshold Crossing Alert) option from the drop-down menu.

The available options are:

- Customize - This option is not supported.
- Disable All - Select this option to disable TCA for all the parameters of a controller. The row colour is (turns) white to indicate that TCA is disabled.
- Enable All - Select this option to enable TCA for all the parameters of a controller. The row colour turns green to indicate that TCA is enabled.

Step 4 The displayed **Warning Thresholds** value is defined in the **Intervals** area.

Step 5 Modify any of the settings described in the following table as needed.

Parameter	Description	Options
Port	(Display only) Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.	
BBE-S-NE	The number of section monitor background block errors on the near-end node.	The valid range for the 15 minute interval is from 0 to 8850600 (Default value is 10000). The valid range for the 1 day interval is from 0 to 8850600 (Default value is 10000).
BBE-S-FE	The number of section monitor background block errors on the far-end node.	The valid range for the 15 minute interval is from 0 to 8850600 (Default value is 10000). The valid range for the 1 day interval is from 0 to 8850600 (Default value is 10000).

Parameter	Description	Options
BBER-S-NE	The number of section monitor background block error ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0). The user needs to enter the value in integer and the value is displayed in decimal till five positions. For example, if the user enters 999, then .00999 is displayed.
BBER-S-FE	The number of section monitor background block error ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0). The user needs to enter the value in integer and the value is displayed in decimal till five positions. For example, if the user enters 999, then .00999 is displayed.
ES-S-NE	The number of section monitor errored seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 500). The valid range for the 1day interval is from 0 to 86400 (Default value is 5000).
ES-S-FE	The number of section monitor errored seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 500). The valid range for the 1day interval is from 0 to 86400 (Default value is 5000).
ESR-S-NE	The number of section monitor errored seconds ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0). The user needs to enter the value in integer and the value is displayed in decimal till five positions. For example, if the user enters 999, then .00999 is displayed.
ESR-S-FE	The number of section monitor errored seconds ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0). The user needs to enter the value in integer and the value is displayed in decimal till five positions. For example, if the user enters 999, then .00999 is displayed.

Parameter	Description	Options
FC-S-NE	The number of section monitor failure count on the near-end node.	The valid range for the 15 minute interval is from 0 to 72 (Default value is 10). The valid range for the 1day interval is from 0 to 6912 (Default value is 40).
FC-S-FE	The number of section monitor failure count on the far-end node.	The valid range for the 15 minute interval is from 0 to 72 (Default value is 10). The valid range for the 1day interval is from 0 to 6912 (Default value is 40).
SES-S-NE	The number of section monitor severely errored seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 500). The valid range for the 1day interval is from 0 to 86400 (Default value is 5000).
SES-S-FE	The number of section monitor severely errored seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 500). The valid range for the 1day interval is from 0 to 86400 (Default value is 5000).
SESR-S-NE	The number of section monitor severely errored seconds ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0). The user needs to enter the value in integer and the value is displayed in decimal till five positions. For example, if the user enters 999, then .00999 is displayed.
SESR-S-FE	The number of section monitor severely errored seconds ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0). The user needs to enter the value in integer and the value is displayed in decimal till five positions. For example, if the user enters 999, then .00999 is displayed.
UAS-S-NE	The number of section monitor unavailable seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 500). The valid range for the 1day interval is from 0 to 86400 (Default value is 5000).
UAS-S-FE	The number of section monitor unavailable seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 500). The valid range for the 1day interval is from 0 to 86400 (Default value is 5000).

Step 6 Click **Apply**.

Step 7 In the Intervals area, select 15 Min or 1 Day, then click **Refresh** to view the updated threshold values.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W ODU PM Thresholds

Purpose	This procedure enables you to provision the ODU PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the ODU PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **ODU** tabs.

Step 3 Select the **TCA** (Threshold Crossing Alert) option from the drop-down menu.

The available options are:

- Customize - This option is not supported.
- Disable All - Select this option to disable TCA for all the parameters of a controller. The row colour is (turns) white to indicate that TCA is disabled.
- Enable All - Select this option to enable TCA for all the parameters of a controller. The row colour turns green to indicate that TCA is enabled.

Step 4 The displayed **Warning Thresholds** value is defined in the **Intervals** area.

Step 5 Modify any of the settings described in the following table as needed.

Parameter	Description	Options
Layer Name	Select a layer name based on which ports and their PM thresholds are displayed.	• path • GFP

Parameter	Description	Options
Port	(Display only) Displays the ODUk port name for which PM thresholds are displayed in the adjacent columns. **Note** ODU ports are displayed for which PM is enabled using **Provisioning** > **Thresholds** > **ODU** tabs.	
BBE-P-NE	The number of path monitor background block errors on the near-end node.	The valid range for the 15 minute interval is from 0 to 8850600 (Default value is 85040). The valid range for the 1day interval is from 0 to 849657600 (Default value is 850400).
BBE-P-FE	The number of path monitor background block errors on the far-end node.	The valid range for the 15 minute interval is from 0 to 8850600 (Default value is 85040). The valid range for the 1day interval is from 0 to 849657600 (Default value is 850400).
BBER-P-NE	The number of path monitor background block errors ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
BBER-P-FE	The number of path monitor background block errors ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
ES-P-NE	The number of path monitor errored seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 87). The valid range for the 1day interval is from 0 to 86400 (Default value is 864).
ES-P-FE	The number of path monitor errored seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 87). The valid range for the 1day interval is from 0 to 86400 (Default value is 864).
ESR-P-NE	The number of path monitor errored seconds ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
ESR-P-FE	The number of path monitor errored seconds ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).

Parameter	Description	Options
FC-P-NE	The number of path monitor failure count on the near-end node.	The valid range for the 15 minute interval is from 0 to 72 (Default value is 10). The valid range for the 1day interval is from 0 to 6912 (Default value is 40).
FC-P-FE	The number of path monitor failure count on the far-end node.	The valid range for the 15 minute interval is from 0 to 72 (Default value is 10). The valid range for the 1day interval is from 0 to 6912 (Default value is 40).
SES-P-NE	The number of path monitor severely errored seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 1). The valid range for the 1day interval is from 0 to 86400 (Default value is 4).
SES-P-FE	The number of path monitor severely errored seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 1). The valid range for the 1day interval is from 0 to 86400 (Default value is 4).
SESR-P-NE	The number of path monitor severely errored seconds ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
SESR-P-FE	The number of path monitor severely errored seconds ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
UAS-P-NE	The number of path monitor unavailable seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 3). The valid range for the 1day interval is from 0 to 86400 (Default value is 10).
UAS-P-FE	The number of path monitor unavailable seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 3). The valid range for the 1day interval is from 0 to 86400 (Default value is 10).

Step 6 Click **Apply**.

Step 7 In the Intervals area, select 15 Min or 1 Day, then click **Refresh** to view the updated threshold values.

Step 8 Return to your originating procedure.

Provision NCS4K-2H-W TCM PM Thresholds

Purpose	This procedure enables you to provision the TCM PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the TCM PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **TCM** tabs.

You must modify 15 Min and 1 Day independently. To do so, choose the appropriate radio button and click **Refresh**.

Step 3 Modify any of the settings described in the following table as needed.

Parameter	Description	Options
TCM	Displays the TCMs configured for the selected ODUk port. **Note** TCMs are displayed for which PM is enabled using **Provisioning** > **Alarm Thresholds** > **TCM** tabs. User can **Enable** or **Disable** the TCA Alerts. User can change the Threshold value.	
BBE-P-NE	The number of path monitor background block errors on the near-end node.	The valid range for the 15 minute interval is from 0 to 8850600 (Default value is 85040). The valid range for the 1 day interval is from 0 to 849657600 (Default value is 850400).

Parameter	Description	Options
BBE-P-FE	The number of path monitor background block errors on the far-end node.	The valid range for the 15 minute interval is from 0 to 8850600 (Default value is 85040). The valid range for the 1 day interval is from 0 to 849657600 (Default value is 850400).
BBER-P-NE	The number of path monitor background block errors ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
BBER-P-FE	The number of path monitor background block errors ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
ES-P-NE	The number of path monitor errored seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 87). The valid range for the 1 day interval is from 0 to 86400 (Default value is 864).
ES-P-FE	The number of path monitor errored seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 87). The valid range for the 1 day interval is from 0 to 86400 (Default value is 864).
ESR-P-NE	The number of path monitor errored seconds ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
ESR-P-FE	The number of path monitor errored seconds ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
FC-P-NE	The number of path monitor failure count on the near-end node.	The valid range for the 15 minute interval is from 0 to 72 (Default value is 10). The valid range for the 1 day interval is from 0 to 6912 (Default value is 40).
FC-P-FE	The number of path monitor failure count on the far-end node.	The valid range for the 15 minute interval is from 0 to 72 (Default value is 10). The valid range for the 1 day interval is from 0 to 6912 (Default value is 40).
SES-P-NE	The number of path monitor severely errored seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 1). The valid range for the 1 day interval is from 0 to 86400 (Default value is 4).

Parameter	Description	Options
SES-P-FE	The number of path monitor severely errored seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 1). The valid range for the 1 day interval is from 0 to 86400 (Default value is 4).
SESR-P-NE	The number of path monitor severely errored seconds ratio on the near-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
SESR-P-FE	The number of path monitor severely errored seconds ratio on the far-end node.	The valid range for the 15 minute and 1 day interval is from 0 to 100000 (Default value is 0).
UAS-P-NE	The number of path monitor unavailable seconds on the near-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 3). The valid range for the 1 day interval is from 0 to 86400 (Default value is 10).
UAS-P-FE	The number of path monitor unavailable seconds on the far-end node.	The valid range for the 15 minute interval is from 0 to 900 (Default value is 3). The valid range for the 1 day interval is from 0 to 86400 (Default value is 10).

Step 4 Click **Apply**.

Step 5 In the Intervals area, select 15 Min or 1 Day, then click **Refresh** to view the updated threshold values.

Step 6 Return to your originating procedure.

Provision NCS4K-2H-W TCA PM Thresholds

Purpose	This procedure enables you to provision the Threshold Crossing Alert (TCA) PM thresholds of the NCS4K-2H-W card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision the TCA PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **PM Thresholds** > **TCA** tabs.

Step 3 Modify any of the settings described in the following table as needed.

Parameter	Description	Options
Port Number	(Display only) Displays the type and address of the controllers in the Rack/Slot/Instance/Port format.	
15 mins	Choose the option from the drop-down menu to set the TCA interval.	The available options are: • Enable All - All the interfaces are set to a TCA interval of 15 minutes. • Disable All - All the set TCA intervals are disabled.
1 Day	Choose the option from the drop-down menu to set the TCA interval.	The available options are: • Enable All - All the interfaces are set to a TCA interval of one day. • Disable All - All the set TCA intervals are disabled.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure.

Provision SRLG on the Ports

Purpose	This procedure provisions Shared Risk Link Groups (SRLGs) on the optics or OTU ports.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision SRLG. The card view appears.

Step 2 Click the **Provisioning** > **Network SRLG** tabs.

Step 3 Provision SRLG on the Optics or OTU ports as needed.

a) Click the **Optics** or **OTU** sub-tab as needed.

b) Select the Controller Name from the drop-down list for which you want to provision SRLG.

c) Double-click the Set field and enter a numeric value to create the number of set(s) under which SRLGs are created. The range is from 1 to 17.

d) Double-click the SRLG fields to enter a numeric value to create SRLGs for the selected port. The SRLG range is from 0 to 4294967294.

The number of available SRLG fields are from 1 to 6.

e) Click **Apply**.

Stop. You have completed this procedure.

Provision Pluggable Port Modules

Purpose	This procedure provisions pluggable port modules (PPMs).
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the NCS4K-2H-W card where you want to provision port modules. The card view appears.

Step 2 Click the **Provisioning** > **Port Modules** tabs.

Step 3 In the Port Modules area, modify any of the settings described in the following table as needed. See Key Features of NCS4K-2H-W Card, on page 7 for information on port mode, mapping, and framing type.

Parameter	Description
Port	Displays the PPM port number.
Service State	Displays the service state of the PPM.

Parameter	Description
Actual Equipment Type	Displays the actual equipment type of the PPM.
Port Mode	Choose the port mode from the Port Mode drop-down list.
Framing Type	Choose the framing type from the Framing Type drop-down list.
Mapping	Choose the mapping from the Mapping drop-down list.
Rate	Choose the rate from the Rate drop-down list. The available rates are: 10GE, 40GE and 100GE.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

CHAPTER 3

Configure LC Priority Shutdown

This chapter describes the procedure to configure the shutdown priority on line cards using CTC.

Table 1: Feature History

Feature Name	Release Information	Feature Description
LC Priority Shutdown	Cisco IOS XR Release 6.5.31	During insufficient power conditions on a chassis, you might want to shut down certain line cards when the power consumption of the chassis exceeds the maximum limit. The LC priority shutdown feature provides a deterministic way of powering down the line cards based on shutdown priorities assigned to the line cards. This leads to significant cost savings. Commands added: • power-mgmt progressive location rack-id • priority location line-card-location card-priority

LC Priority Shutdown

The LC priority shutdown feature allows you to assign a priority to the line cards. The priority is used to determine the order in which the line cards must be shut down when the power consumption of the chassis exceeds the maximum limit. You can choose a priority from 0 to 19. If a priority is not set for a line card, a default value of 20 is set. The line card with the higher priority is shut down first. If the same priority is set for two or more cards, the line card in the higher slot number is shut down first.

In Release 6.5.31, this feature is not applicable during a chassis or line card reload.

This feature is not supported on fabric cards.

The following alarms are associated with this feature:

- **Total power draw nearing total power capacity,insert PEMS to avoid LC shutdown**-This alarm is raised when the chassis power consumption is greater than or equal to (the total power capacity – 100). Use the **show alarms brief system active** command to view this alarm.
- **Card shutdown by Progressive power-mgmt mode**- This transient condition is raised when the chassis power consumption is greater than or equal to the (total power capacity - 80). The line cards are shut down based on the priority assigned. Use the **show alarms brief system history** command to view this transient condition.

Configure LC Priority Shutdown

Purpose	This procedure enables you to enable and configure the shutdown priority on line cards using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click the **Provisioning** > **General** > **LC Priority Shutdown** tabs.

Step 2 To enable the feature, check the **Priority Shutdown** checkbox.

Step 3 Enter the priority for the line card in the **Priority** field.

You can choose a priority from 0 to 19. If the same priority is set for two cards, the card in the higher slot number is shut down first. By default, a priority of 20 is assigned to all the line cards when the feature is enabled.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

CHAPTER 4

Configure AINS

This chapter describes the procedure to configure the AINS.

AINS Support for Controllers

After the completion of a maintenance window, the controller can be removed from the maintenance state without manual intervention by configuring the Automatic-In-Service (AINS) state with a soak time period. After the expiry of the soak time period, the state automatically goes to the normal or the In-Service state.

AINS can be set or cleared on the controller using the **automatic-in-service controller optics** *R/S/I/P* **hours** *x* **minutes** *y* command in the EXEC XR mode.

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

The soak time can be configured when the controller is moved to the AINS state. The minimum soak time is 0 hours 15 minutes and the maximum is 48 hours. The soak time can be configured in intervals of 15 minutes. If a soak time is not specified, it defaults to eight hours. If the soak time is set to 0 using the **automatic-in-service controller** *controller-name R/S/I/P* **hours 0 minutes 0** command , the AINS configuration on the controller is cleared.

The AINS configuration can be viewed using the **show controllers** *controller-name R/S/I/P* command.

```
RP/0/RP0:hostname#show controllers odu2 0/6/0/2
Tue Aug 14 04:02:09.591 UTC

Port                                            : ODU2 0/6/0/2
Controller State                                : Up
Inherited Secondary state                       : Normal
Configured Secondary state                      : Automatic-In-Service
Derived State                                   : Automatic-In-Service
Loopback mode                                   : None
BER Thresholds                                  : SF = 1.0E-6  SD = 1.0E-7

Performance Monitoring                          : Disable

Path Monitoring Mode                            : Non-Intrusive Monitor
PM TIM-CA state                                 : 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
     SAPI  ASCII                                : P M - T R C   S A P I - S E C
     SAPI  HEX                                  : 00504D2D54524320534150492D534543
     DAPI  ASCII                                : P M - T R C   D A P I - S E C
     DAPI  HEX                                  : 00504D2D54524320444150492D534543
     OPERATOR SPECIFIC ASCII                    : PM-TRC OPERATOR SPECIFIC SECTION
     OPERATOR SPECIFIC HEX                      :
504D2D545243204F50455241544F522053504543494649432053454354494F4E
ODU TTI Expected

Owner                                           : All
Resource State                                  : ODU Cross Connection

AINS Soak                                       : Running
AINS Timer                                      : 0h, 15m
AINS remaining time                             : 898 seconds
```

The priority amongst the secondary administrative states are Maintenance > Automatic In-Service > In-Service (Normal). When the controller is put into maintenance, the soak timer is automatically paused and the soak timer status is moved to pending.

```
RP/0/RP0:hostname#configure
Tue Aug 14 04:02:54.242 UTC
RP/0/RP0:hostname(config)#controller odu2 0/6/0/2 secondary-admin-state maintenance
RP/0/RP0:hostname(config)#commit
Tue Aug 14 04:03:00.752 UTC
RP/0/RP0:hostname(config)#end
RP/0/RP0:hostname#sh controllers odu2 0/6/0/2
Tue Aug 14 04:03:03.810 UTC
Port                                            : ODU2 0/6/0/2
Controller State                                : Up
Inherited Secondary state                       : Normal
Configured Secondary state                      : Maintenance
Derived State                                   : Maintenance
Loopback mode                                   : None
BER Thresholds                                  : SF = 1.0E-6  SD = 1.0E-7
Performance Monitoring                          : Disable
Path Monitoring Mode                            : Non-Intrusive Monitor
PM TIM-CA state                                 : 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
     SAPI  ASCII                                : P M - T R C   S A P I - S E C
     SAPI  HEX                                  : 00504D2D54524320534150492D534543
     DAPI  ASCII                                : P M - T R C   D A P I - S E C
     DAPI  HEX                                  : 00504D2D54524320444150492D534543
     OPERATOR SPECIFIC ASCII                    : PM-TRC OPERATOR SPECIFIC SECTION
     OPERATOR SPECIFIC HEX                      :
504D2D545243204F50455241544F522053504543494649432053454354494F4E
```

```
ODU TTI Expected
Owner                                           : All
Resource State                                  : ODU Cross Connection
AINS Soak                                       : Pending
AINS Timer                                      : 0h, 15m
AINS remaining time                             : 847 seconds
```

After the completion of maintenance, the soak timer restarts and the status is moved to running. After the expiry of the soak time, the controller is moved to the in-service state.

```
RP/0/RP0:hostname#configure
Tue Aug 14 04:03:08.630 UTC
RP/0/RP0:hostname(config)#no controller odu2 0/6/0/2 secondary-admin-state
RP/0/RP0:hostname(config)#commit
Tue Aug 14 04:03:16.396 UTC
RP/0/RP0:hostname(config)#end
RP/0/RP0:hostname#sh controllers odu2 0/6/0/2
Tue Aug 14 04:03:18.831 UTC
Port                                            : ODU2 0/6/0/2
Controller State                                : Up
Inherited Secondary state                       : Normal
Configured Secondary state                      : Automatic-In-Service
Derived State                                   : Automatic-In-Service
Loopback mode                                   : None
BER Thresholds                                  : SF = 1.0E-6  SD = 1.0E-7
Performance Monitoring                          : Disable
Path Monitoring Mode                            : Non-Intrusive Monitor
PM TIM-CA state                                 : 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
     SAPI  ASCII                                : P M - T R C   S A P I - S E C
     SAPI  HEX                                  : 00504D2D54524320534150492D534543
     DAPI  ASCII                                : P M - T R C   D A P I - S E C
     DAPI  HEX                                  : 00504D2D54524320444150492D534543
     OPERATOR SPECIFIC ASCII                    : PM-TRC OPERATOR SPECIFIC SECTION
     OPERATOR SPECIFIC HEX                      :
504D2D545243204F50455241544F5220535045434946494320534543354494F4E
ODU TTI Expected
Owner                                           : All
Resource State                                  : ODU Cross Connection
AINS Soak                                       : Running
AINS Timer                                      : 0h, 15m
AINS remaining time                             : 845 seconds
```

If a traffic impacting alarm is raised on the controller, the AINS soak timer is reset to the previously configured value or to eight hours if AINS was not previously configured. To transition from the AINS state to the in-service state, a clean soak period is mandatory with no traffic impacting alarms on the controller. New alarms are suppressed when the controller is in AINS state.

Inheritance of AINS settings

- The AINS state is inherited by child controllers (OTU and ODU) from the parent controller .
- Low order ODUs inherit configured soak timer values.
- If a child controller is configured first with a higher soak timer value and then the parent controller is configured with a lower soak timer value, then the child controller inherits the parent value.

- If the parent controller is configured first with a lower value and then the child controller is configured with a higher value, then the parent and child controllers retain their locally configured values and there is no inheritance.
- If the child controller is configured first with a lower value and then parent controller is configured with a higher value, then the child controller inherits the parent controller value.
- If the parent controller is configured with a higher value and then the child controller is configured with a lower value, the value is rejected as the soak time can be locally configured on the child controller but cannot be lesser than the parent controller.

Configure AINS

Purpose	This procedure enables you to configure and view AINS settings on a controller using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the card where you want to provision AINS for the controllers.

The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > *controller-name* tabs.

controller-name :

Optics, OC, STS, STM, VC, Ethernet, OTU, ODU.

The Optics is the parent controller. The service state is inherited by the child controllers.

Step 3 Choose IS,AINS from the admin state drop-down list.

Step 4 Set the soak time in hours and minutes in the soak time field.

The soak time can be set in intervals of 15 minutes to a maximum of 48 hours. The soak time configured locally on the child controllers cannot be lesser than the parent controller.

Step 5 Click **Apply**.

Step 6 To view the AINS settings on the controller, click the **Maintenance** > **AINS Soak** tabs.

Stop. You have completed this procedure.

CHAPTER 5

Configure Line Cards Using CTC

This section provides the CTC procedures to configure line cards.

Understand ODU and ODU Cross Connections

In the case of channelization, ODU is created as a sub controller of an OTU controller.

Optical Channel Data Unit (ODU) contains information for maintenance and operational functions to support optical channels. ODU Over Head (OH) information is added to the ODU payload to create the complete ODUk. The ODUk OH consists of portions dedicated to the end-to-end ODUk path and to six levels of tandem connection monitoring. The ODUk path OH is terminated where the ODUk is assembled and disassembled. The TCM OH is added and terminated at the source and sink to the corresponding tandem connections.

ODU cross connection is an end-to-end channel between two OTN/Client ports in OTN network within NCS4k node.

The NCS 4000 network element supports the following types of ODU cross connections:

1. Unidirectional point to point
    - 1+1 unidirectional SNC/N, SNC/I protection without an APS protocol
    - 1+1 unidirectional SNC/N, SNC/I protection with an APS protocol
2. Bidirectional point to point
    - 1+1 bidirectional SNC/N, SNC/I protection with an APS protocol

Client Port Optimization in NCS4K-4H-OPW-QC2 Cards

The number of QSFP+ pluggables used on the client and network side of the NCS4K-4H-OPW-QC2 card can be optimised.

To achieve a total bandwidth of 400G, the CFP2 ports and client ports can be configured in any one of the configurations shown in the following tables:

Note A total of five QSFP+ pluggables, each supporting 40G are used on the client side.

Table 2: Port Configuration 1 on NCS4K-4H-OPW-QC2 Cards

Bandwidth (Total of 400G)	CFP2 (Port 10)	CFP2 (Port 11)	Client Ports (0, 1, 2, 3, or 4)	Client Ports (5, 6, 7, 8, or 9)
220G	100G	-	3 QSFP+ x (4 x 10G) or 3 QSFP+ x 40G	-
180G	-	100G	-	2 QSFP+ x (4 x 10G) or 2 QSFP+ x 40G

Table 3: Port Configuration 2 on NCS4K-4H-OPW-QC2 Cards

Bandwidth (Total of 400G)	CFP2 (Port 10)	CFP2 (Port 11)	Client Ports (0, 1, 2, 3, or 4)	Client Ports (5, 6, 7, 8, or 9)
180G	100G	-	2 QSFP+ x (4 x 10G) or 2 QSFP+ x 40G	-
220G	-	100G	-	3 QSFP+ x (4 x 10G) or 3 QSFP+ x 40G

To configure the ports, see Configure an OTN Controller Using CTC, on page 51.

Laser Quelching

Squelching supports the laser shutdown of the client signal when there is a failure in the OTN network.When the network is down, squelching saves power. The Squelched alarm is raised on the client controller when the laser is squelched.

You can configure the squelch hold-off timer. After the expiry of the hold-off timer, the laser is squelched.

Squelching is supported on the NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 cards.

Idle Frame

Idle frames are used to prevent unnecessary switching at the client end. When there is a fault in the client signal, valid idles frames are sent in the downstream direction on the ten GigE, forty GigE, or hundred GigE client interface instead of raising an AIS or LF. This prevents unnecessary switching at the client end.

You can configure the idle frame hold-off timer. When the hold-off timer is running, idle frames are sent to the downstream client router. After the expiry of the hold-off timer, idle frames are no longer sent in the downstream direction. Instead, the upstream router communicates the incidence of a fault that has occurred using applicable alarms to the client router in the downstream dirction.

Idle frames are supported on the ethernet mapper ODUs of the NCS4K-4H-OPW-QC2 card.

Configure Line Cards Using CTC

This section provides the CTC procedures to configure line cards.

Configure an OTN Controller Using CTC

Purpose	This procedure enables you to create an OTN controller for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double-click the line card.

Step 2 Click the **Provisioning** > **Port Modules** tabs.

Step 3 Perform the following steps for the port number on which you want to configure the controller interface :

a) Click the **Port Mode** column and select the port mode type from the drop down list.
b) Click the **Framing Type** column and select the OPU type from the drop down list.
c) Click the **Mapping** column and select the mapping type from the drop down list.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

Configure Controller Optics for OTN Controller Using CTC

Purpose	This procedure enables you to update the default parameters of controller optics, for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double-click the line card.

Step 2 Click the **Provisioning** > **Controllers** > **Optics** tabs.

Step 3 Perform the following (as required) to update the parameters of Controller Optics you want to configure:

a) Click the **Admin State** column and select the administrative state of the controller from the drop down list.

Note Primary and Secondary states are shown as Admin state in CTC.

b) Check the **Enable PM** check box.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

Configure 100MHz Grid Spacing for NCS4K-4H-OPW-QC2 Line Card Using CTC

Purpose	This procedure enables you to update the grid spacing wavelength for the NCS4K-4H-OPW-QC2 line card, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Table 4: Feature History

Feature Name	Release Information	Feature Description
100MHz Grid Spacing for NCS4K-4H-OPW-QC2 card	Cisco IOS XR Release 6.5.33	In addition to the 50GHZ flex-grid-spacing, you can now configure 100MHz flex-grid-spacing on the CFP2 trunk ports of the NCS4K-4H-OPW-QC2 card. The setup can be done by Cisco Transport Controller (CTC) or CLI. With 100MHz flex-grid-spacing, you can configure up to 761 different wavelengths; which is more than 96 wavelengths that can be done with 50GHZ flex-grid-spacing.

The trunk ports 10 and 11 with coherent CFP2 optics in the NCS4K-4H-OPW-QC2 line card currently support 50GHz grid spacing. However, the coherent CFP2 optics supports 100MHz grid spacing. From Release 6.5.33, you can configure 100MHz flex grid spacing. The 100MHz grid spacing enables you to configure the frequencies with a granularity of 7 digits, and therefore 761 different wavelengths can be configured on the colored optics, whereas 50GHz grid spacing can support only 96 wavelengths.

You can also configure the 100MHz grid spacing through CLI. See Configure 100MHZ Flex Grid for NCS4K-4H-OPW-QC2 Line Card, on page 235.

Procedure

Step 1 In the Node view, double-click the NCS4K-4H-OPW-QC2 line card.

Step 2 Click the **Provisioning** > **Controllers** > **Optics** tabs.

Step 3 Perform the following for the Optics 0/0/0/10 and Optics 0/0/0/11 controllers Optics that you want to configure:

a) Choose the **Admin State** as OOS, DSBLD, or OOS, MT.
b) Choose the **Grid Type** as 100MHz.
c) Choose the required **Wavelength**.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

Configure OTU for OTN Controller Using CTC

Purpose	This procedure enables you to update the default parameters of OTUk for OTN controller, for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double-click the line card.

Step 2 Click the **Provisioning** > **Controllers** > **OTU** tabs.

Step 3 Perform the following (as required) to update the parameters of the OTU you want to configure:

a) Click the **Admin State** column and select the administrative state of the controller from the drop down list.

Note Primary and Secondary states are shown as Admin state in CTC.

b) Click the **FEC** column and select FEC value from drop down list. Available options are None and Standard.

c) Check the **GCC0** check box to enable GCC on the corresponding controller.

d) Check the **Enable PM** check box.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

Configure ODU for OTN Controller Using CTC

Purpose	This procedure enables you to update the default parameters of ODUk for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double-click the line card.

Step 2 Click the **Provisioning** > **Controllers** > **ODU** tabs.

Step 3 Perform the following (as required) to update the parameters of the ODU you want to configure:

a) Click the **Admin State** column and select the administrative state of the controller from the drop down list.

Note Primary and Secondary states are shown as Admin state in CTC.

b) Check the **GCC1** check box to enable GCC on the corresponding controller.

c) Check the **Enable PM** check box to enable performance monitoring.

d) Click the **TSG** column and select TSG (Time Slot Granularity) value from drop down list. Available options are 1.25 to 2.5.

Note Time granularity is optional for user.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

Configure Squelch for ODU Controller Using CTC

Purpose	This procedure enables you to configure the squelch settings on an ODU controller of the NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, or NCS4K-4H-OPW-QC2 card using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the card where you want to provision squelch for the controllers.

The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > **ODU** tabs.

Step 3 Choose Laser Squelch from the Fault Signalling drop-down list.

Step 4 Set the hold-off time in ms in the Hold-off Timer field.

The range for the hold-off timer is 20ms to 10000ms.

Step 5 Click **Apply**.

Stop. You have completed this procedure.

Configure Idle Frame for ODU Controller Using CTC

Purpose	This procedure enables you to configure the idle frame settings on an ODU controller of the NCS4K-4H-OPW-QC2 card using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, double-click the card where you want to provision squelch for the controllers.

The card view appears.

Step 2 Click the **Provisioning** > **Controllers** > **ODU** tabs.

Step 3 Choose Idle Frame from the Fault Signalling drop-down list.

Step 4 Set the hold-off time in ms in the Hold-off Timer field.

The range for the hold-off timer is 20ms to 10000ms.

Step 5 Click **Apply**.

Stop. You have completed this procedure.

Configure Trace Monitoring for OTN Controller Using CTC

Purpose	This procedure enables you to configure trace monitoring for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node view, double-click the line card.

Step 2 Click the **Provisioning** > **Trace Monitoring** tabs.

Step 3 From the **Controller Name** drop-down list, choose a name of the controller.

Step 4 In the Transmit area, perform following steps:

a) Select **Operator Specific Type** to specify the data type for the transmit string. Available options are ASCII and Hex (1 byte).
b) Enter the transmit string in the **Operator String** field.
c) Click **Hex Mode or ASCII Mode** to convert the current transmit string to hexadecimal or ASCII data.

Step 5 In the Expected area, perform following steps:

a) Select **Operator Specific Type** to specify the data type for the expected string. Available options are ASCII and Hex (1 byte).
b) Enter the expected string in the **Operator String** field.
c) Click **Hex Mode or ASCII Mode** to convert the current expected string to hexadecimal or ASCII data.

Step 6 Click **Apply**.

Stop. You have completed this procedure.

Configure the Alarm Threshold Values for OTN Controllers Using CTC

Purpose	This procedure enables you to configure the alarm threshold values of a controller, for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*. Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double-click the line card.

Step 2 Click the **Provisioning** > **Alarm Thresholds** > **OTU** tabs.

Step 3 Click the **OTU** tab and seect the SF BER and SD BER parameters, to configure threshold values of an OTU.

Parameter	Description
SF BER	Sets the signal fail bit error rate. The range is for NCS4K-20T-O-S is from 1E-6 to 1E-9. The default value is 6. The range for other cards is from 1E-5 to 1E-9. The default value is 5.
SD BER	Sets the signal degrade bit error rate. The range is from 1E-3 to 1E-9. The range is for NCS4K-20T-O-S is from 1E-6 to 1E-9. The default value is 7. The range for other card is from 1E-5 to 1E-9. The default value is 7.

Step 4 Click the **ODU** tab and modify the following settings, to configure threshold values of an ODU.

Parameter	Description
SF BER	Sets the signal fail bit error rate. The range is for NCS4K-20T-O-S is from 1E-6 to 1E-9. The default value is 6. The range for other cards is from 1E-5 to 1E-9. The default value is 5.
SD BER	Sets the signal degrade bit error rate. The range is from 1E-3 to 1E-9. The range is for NCS4K-20T-O-S is from 1E-6 to 1E-9. The default value is 7. The range for other cards is from 1E-5 to 1E-9. The default value is 7.

Step 5 Click **Apply**.

Stop. You have completed this procedure.

Configure the Network SRLG for OTU and Controller Optics Using CTC

Purpose	This procedure enables you to configure the Shared Resource Link Group (SRLG) for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node view, double-click the line card.

Step 2 Click the **Provisioning** > **Network SRLG** tab.

Step 3 To configure network SRLG, click the **Optics/ OTU** tab and perform the following steps:

a) From the **Controller Name** drop-down list, select the controller.
b) Double click **Set** column and enter the value of Set.
c) Double click the **SRLG 1** column and enter value of SRLG 1.

Repeat this step for columns SRLG2, SRLG3, SRLG4, SRLG5, and SRLG 6.

Note Click **Add** and repeat steps 3b and 3c, for configuring more SRLG's on the controller.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

Connect Backplane/Regeneration of line cards Using CTC

Purpose	This procedure enables you to connect Backplane/Regeneration of NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, and NCS4K-2H10T-OP-KS line cards, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node view, double-click the line card.

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

Step 3 Click the **Backplane** radio buttons and perform the following steps in the screen that appears:

a) From the Backplane drop-down list, choose the port number of the card.

Note The port number that appears in the Backplane drop-down list depends on the card provisioned in the chassis.

- NCS4K-2H-W 2 or 3
- NCS4K-20T-O-S (0-9) or Port (10-19)
- NCS4K-24LR-O-S
- NCS4K-2H10T-OP-KS

The card must be the following combination

- NCS4K-20T-O-S and NCS4K-2H-W
- NCS4K-2H-W and NCS4K-20T-O-S
- NCS4K-2H-O-K9 and NCS4K-2H-W
- NCS4K-2H-W and NCS4K-2H-O-K9
- NCS4K-2H10T-OP-KS and NCS4K-2H-W

b) From the Peer Card drop-down list, choose the location of the card in the Rack/Slot/Instance/Port format.

c) From the Peer Card Backplane drop-down list, choose a value.

Note It depends on the peer card provisioned in the chassis.

- NCS4K-2H-O-K9 0 or 1
- NCS4K-2H-W 2 or 3
- NCS4K-20T-O-S (0-9) or Port (10-19)
- NCS4K-2H10T-OP-KS

d) Click **Apply**.

Step 4 Click the **Regeneration** radio button and perform the following steps in the screen that appears:

Note The regeneration is applicable only with NCS4K-2H-W card.

a) From the Port drop-down list, choose port number of the card.

b) Click **Apply**.

Stop. You have completed this procedure.

Upgrade to 400G Fabric Card Using CTC

Purpose	This procedure provides instructions for upgrading from a 200G FC (NCS4016-FC-M) to a 400G FC (NCS4016-FC2-M).
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In Node View , select the **Maintenance** tab.

Step 2 Click **Fabric Upgrade** to get the current Fabric Details. The table displays the following details:

Title	Description
Plane ID	Displays all the plane IDs.
Plane Admin Status	Displays current admin status of all planes. The admin status can either be Up or Down.
Plane Oper Status	Displays current operational status of all planes. The operational status can either be Up or Down.
Hardware Status	Displays hardware status of all Fabrics. The possible states are IS-NR and OOS-AU, indicating In-service and Out-of-service, respectively.
Product ID	Displays the Product ID of all fabrics. The product-id for the 200G fabric card is NCS4016-FC-M; for the 400G fabric card is NCS4016-FC2-M.

Note The Plane Admin status and the Plane Oper status need to be Up for all the Plane IDs before proceeding with the fabric card upgrade.

The Fabric Details table is for display purpose only, the displayed elements cannot be selected.

Step 3 Click **Refresh Fabric Details Table** , to get the updated table.

Step 4 The **Upgrade Wizard**, provides the console for upgrading the fabric. Select the fabric plane from the **Available Fabrics** drop-down menu.
Once this selection is done, the Available Fabrics option is grayed-out until the whole upgrade process is complete.

Step 5 Click **Next** (referred to as Step-1 in the Upgrade Wizard) to shutdown the selected fabric plane; click **Yes** on the Confirmation Dialog.
A message is displayed to indicate that the selected plane was successfully shutdown.

Step 6 Click **Next** (referred to as Step-2) to shutdown the corresponding fabric card.

Step 7 Replace the 200G FC with a 400G FC and click **Next** (referred to as Step 3 in the Upgrade Wizard).

The **Revert** option appears after Step-1. It allows the user to undo the action performed in the previous step. Be careful not to use this option after replacing the card. Clicking **Revert** will un shut the newly inserted card.

Step 8 Wait for the Hardware Status column of the relevant Plane ID, in the fabric details table to display IS-NR, indicating in-service. Click **Next** (referred to as Step 4 in the Upgrade Wizard).

Step 9 Click **Next** to upgrade the FPD device for the selected fabric (referred tp as Step 5 in the Upgrade Wizard).

Step 10 On choosing to upgrade the FPD device, a message is displayed recommending the user to check the FPD status under the **Maintenance** > **Software** > **FPD Upgrade** tab.

The user has an option to click **Skip** to proceed without upgrading the FPD devices. The user can revisit the **FPD Upgrade** tab anytime to upgrade the FPDs.

Step 11 Click **Finish**, to activate (no shutdown) the fabric plane (referred to as Step 6 in the Upgrade Wizard).
The **Available Fabrics** drop-down menu is now available, wherein the user can select another fabric card.

Step 12 The **Output Window** , displays the details of the performed actions. The user can extract this log by clicking the **Export Log** button and saving the information to a desired location.

What to do next

Repeat the procedure to upgrade all the 200G FCs to 400G FCs. Mixed mode (where 200G FCs and 400G FCs co-exist) is recommended only while performing the upgrade . The user is required to upgrade all the FCs to 400G before making any configuration change(s).

Upgrade FPD using CTC

Purpose	This procedure enables you to upgrade Field-programmable device (FPD) .
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Maintenance** tab.

Step 2 Click the **Software** > **FPD Upgrade** tab.

Step 3 To Upgrade FPD, perform the following steps:

a) Click **Reset** to refresh the drop-down lists.

b) From **Location** drop-down list, select the card/RP.

c) From **FPD Device** drop-down list, select the FPD that needs upgrade.

d) For forced upgrade/downgrade of all FPD's, check the **Force** checkbox.

Note Skip this step, if forced upgrade/downgrade of all FPD's is not required.

e) Click **Upgrade**.

f) Click **Reload**, if card/RP reload is required to complete the FPD upgrade.

Note Reload is traffic impacting operation and should be carried in planned maintenance window.

To perform non traffic impacting FPD upgrade for fabric card refer Non Disruptive FPD Upgrade for Fabric Card using CTC, on page 63.

To perform non traffic impacting FPD upgrade for RP refer Non Disruptive FPD Upgrade for Route Processor using CTC, on page 64.

Stop. You have completed this procedure.

Non Disruptive FPD Upgrade for Fabric Card using CTC

Purpose	This procedure enables you to upgrade FPD for fabric card without impacting traffic .
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Maintenance** tab.

Step 2 Click the **Software** > **FPD Upgrade** tab.

Step 3 To upgrade the FPD, perform following steps:

a) Click **Reset** to refresh the drop-down lists.
b) From **Location** drop-down list, select the required fabric card.
c) From **FPD** drop-down list, select a FPD.

   For forced upgrade/downgrade of all FPD's, check the **Force** checkbox.

d) Click **Upgrade**.

Step 4 Click **Fabric Plane** tab.

Step 5 Click **Fabric Plane Maintenance**.

Step 6 In the **Fabric Plane Maintenance** dialog box, perform the following steps to shut down the fabric plane:

a) From the **Plane ID** drop down list, select the fabric plane of the selected fabric card.
b) From the **Admin State** drop down list, set the state of the selected fabric plane as OOS/DSBLD (Out Of Service/Disabled).
c) Click **Apply**.
   This will shut down the fabric plane.

Step 7 Click the **Software** > **FPD Upgrade** tabs.

Step 8 Select the fabric card whose fabric plane was shut down in Step6.

Step 9 Click **Reload**.
This will reload the selected fabric card. No traffic impact shall be observed because of 3+1 fabric card redundancy.

Step 10 Wait for 2 minutes.

Step 11 Click **Fabric Plane** tab.

Step 12 Click **Fabric Plane Maintenance**.

Step 13 In the **Fabric Plane Maintenance** dialog box, perform the following steps to make the fabric plane operational again:

a) From the **Plane ID** drop down list, select the fabric plane that was shut down in Step6.
b) From the **Admin State** drop down list, set the state of the selected fabric plane as IS (In Service).
c) Click **Apply**.

Note Repeat these steps 4 to 13 for other fabric cards.

Stop. You have completed this procedure.

Non Disruptive FPD Upgrade for Route Processor using CTC

Purpose	This procedure enables you to upgrade FPD image for Route Processor (RP) without impacting traffic.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Maintenance** tab.

Step 2 Click the **Software** > **FPD Upgrade** tabs.

Step 3 Perform the following steps, to upgrade FPD's for Standby RP :

a) Click **Reset** to refresh the drop-down lists.
b) From **Location** drop-down list, select the Standby RP.
c) From **FPD** drop-down list, select a FPD.

For forced upgrade/downgrade of all FPD's, check the **Force** checkbox.

d) Click **Upgrade**.
e) Click **Reload**, if RP reload is required to complete FPD upgrade.

Step 4 Perform the following steps, to upgrade FPD's for Active RP :

a) Click **Reset** to refresh the drop-down lists.
b) From **Location** drop-down list, select the Active RP.
c) From **FPD** drop-down list, select the FPD.

For forced upgrade/downgrade of all FPD's, check the **Force** checkbox.

d) Click **Upgrade**.
e) Click **Reload**, if RP reload is required to complete FPD upgrade.

Note This would result in RP switchover, standby RP taking over as active RP, and upgrade of FPD's for both RP's.

Stop. You have completed this procedure.

CHAPTER 6

Configure Circuits

The OTN circuits allow you to setup end to end circuits from the origin to a destination network element. The Optical Channel Trail circuits allow you to create circuits in a network where the NCS 4000 series node is connected to ONS 15454, ONS 15454 M2, or ONS 15454 M6 nodes. This chapter provides the CTC procedures to configure the circuits.

Understand OTN Circuits

An OTN circuit provides the ability to aggregate different types of traffic such as Ethernet, SONET or SDH, and packet over OTN at different data rates such as 1.25, 2.5, 10, 40, or 100 GBit per second. This aggregated traffic is transported by network elements that acts as OTN cross connections.

ODUk controllers can be cross connected with controllers of the same rate in an OTN circuit by a fabric card. The following network applications are associated with OTN network elements:

- End-to-end circuits from any rate or any payload client service
- End-to-end circuit from a client service versus the OTN (OTUk) network
- Aggregation of OTN traffic (OTUk)

Understand Circuit Diversity

This feature enables the user to create a circuit that is diverse from an existing circuit in the network. This is to increase survivability and availability in case of link failures.

During the computation of a diverse circuit, the GMPLS algorithm attempts to find a shared resource link group (SRLG) diverse path. If the path is not available, node and link diversity is used to compute the new path. Enabling circuit diversity on an existing circuit causes re-signaling of the circuit.

The following restrictions are applicable to ODU TUNNEL circuits:

- The diverse circuit must have the same head node.
- Supported only for 1+0 circuits.
- If a diverse path is not found, the circuit is not created.

This feature is supported on the NCS4K-4H-OPW-QC2 card.

Understand OSPF

Open Shortest Path First (OSPF) is a routing protocol designed to run an autonomous system. It maintains an identical database describing the topology of an autonomous system. From the identical database, a shortest path-tree calculates the routing table. OSPF-TE allows controlling the data packet's path.

OSPF provides following features:

- Routing of area.
- Routing of protection.
- Minimizing the routing protocol traffic.

Understand MPLS TE

MPLS TE learns the topology and resources available in a network and then maps traffic flows to respective paths based on resource requirements and network resources, for example, bandwidth. MPLS TE builds a unidirectional tunnel from a source to a destination in the form of a label switched path (LSP), which is then used to forward traffic. Tunnel head end or tunnel source is the point where the tunnel begins, the tunnel tail end or tunnel destination is the node where the tunnel ends .

Understand Tandem Connection Monitoring

Tandem Connection Monitoring (TCM) layer is used for protection applications, for example, APS. The path layer can be used for protection, however, it can be influenced by errors that occur outside a given operators network and cause undesired protection switch events to occur within their network. Since TCM can isolate a service to a given domain, it can be used to trigger protection applications and avoid such issues.

Six levels of TCM, each with various modes of operation, are provided to allow for simultaneous use for different monitoring applications along any each and every individual ODU trail. These applications include: segment protection, administrative domain monitoring, service monitoring, fault localization, verification of delivered quality of service, delay/latency measurements and adjacency discovery.

Understand Automatic Protection Switching

Automatic Protection Switching (APS) is a protection mechanism for OTN networks that enables OTN connections to switch to another circuit when a circuit failure occurs. A protect circuit serves as the backup circuit for the working circuit. When the working circuit fails, the protect circuit quickly assumes its traffic load.

In a linear protection architecture, protection switching occurs at the two distinct endpoints of a protected circuit. For a given direction of transmission, the head-end or the tail-end of the protected signal performs a bridge function, and places a copy of a normal traffic signal onto a protection entity when required. The tail-end or the head-end performs a selector function, where it is capable of selecting a normal traffic signal either from its usual working entity, or from a protection entity.

The widely used protection mechanism is the 1+1 architecture. Here, a single normal traffic signal is protected by a single protection entity. The bridge at the head-end is permanent. Switching occurs entirely at the tail-end.

In the case of bidirectional transmission, it is possible to choose either unidirectional or bidirectional switching. With unidirectional switching, the selectors at each end are fully independent. With bidirectional switching, an attempt is made to coordinate the two ends so that both have the same bridge and selector settings, even for a unidirectional failure. Bidirectional switching always requires an APS and/or protection communication channel (PCC) to coordinate the two endpoints. Unidirectional switching can protect two unidirectional failures in opposite directions on different entities.

Hierarchy in APS

There are different levels of priority that can be set for the path to switch from a working circuit to the protect circuit (or vice-versa). The hierarchy levels are (listed priority-wise, with lockout having the highest priority):

- Lockout - the path continues to be in the working circuit, even if a failure is detected in the working circuit, switch to the protect circuit is not permitted. If the path is currently using the protect circuit, then it automatically switches back to the working circuit.
- Forced switch - forces a switch from the protect circuit to the working circuit (even when the protect circuit is down, this scenario can happen during a maintenance activity).
- Manual switch - manually switches from the working circuit to the protect circuit or from the protect circuit to the working circuit.
- Exercise - enables the APS protocol.

  m

Understand Subnetwork Connection

Subnetwork Connection Protection (SNCP) configurations provide duplicate fiber paths for a circuit. Working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem occurs with the working traffic path, the receiving node switches to the path coming from the opposite direction. The node at the end of the path and the intermediate nodes in the path select the best traffic signal. The virtual container is not terminated at the intermediate node, instead, it compares the quality of the signal on the two incoming ports and selects the better signal.

SNC can be classified into three types:

- SNC/I (inherent) - Protection switching is triggered by defects detected at the ODUk link connection.
- SNC/N (non-intrusive) - Protection switching is triggered by a non-intrusive monitor of the ODUkP trail.
- SNC/S (sublayer) - Protection switching is triggered by defects detected at the ODUkT sublayer trail (TCM). An ODUkT sublayer trail is established for each working and protection entity.

Understand 1+R Protection

1+R protection mechanism is SNC-based. In case of work path failure, the circuit uses the restore path. Here, the protect path is not defined by the user (as in case of other protection mechanisms). The restore path is defined by the GMPLS protocol. To enable GMPLS, see Enabling GMPLS Using CTC, on page 74

1+1+R

In 1+1+R protection mechanism, a circuit is protected by two redundant paths, one is the protect path and the other one is the restore path. When a failure occurs on the working and the protect paths, then the restore path takes over. Wait to Restore (WTR) timers are available on both the working and protect paths. Restoration path signalling is triggered as soon as a defect is detected on either of the paths (working or protect). So, when the working path fails, the traffic shifts to the protect path. In this period of time, the restore path is ready to take over as soon as the protect path fails too; the switchover time is less than 50ms.

These are the limitations for 1+1+R protection mechanism:

- Unidirectional protection type is not supported.
- Manual switch to restore is not supported.

Understand ISSU Upgrade

In-Service Software Upgrade (ISSU) is a technique that updates the software packages on a network element without affecting the traffic. By using ISSU, you can deploy new Cisco IOS XR Software images that supports new software features and services. The Cisco IOS XR ISSU capability extends Cisco high availability innovations for minimizing planned downtime for service provider networks.

Understand GCC Management

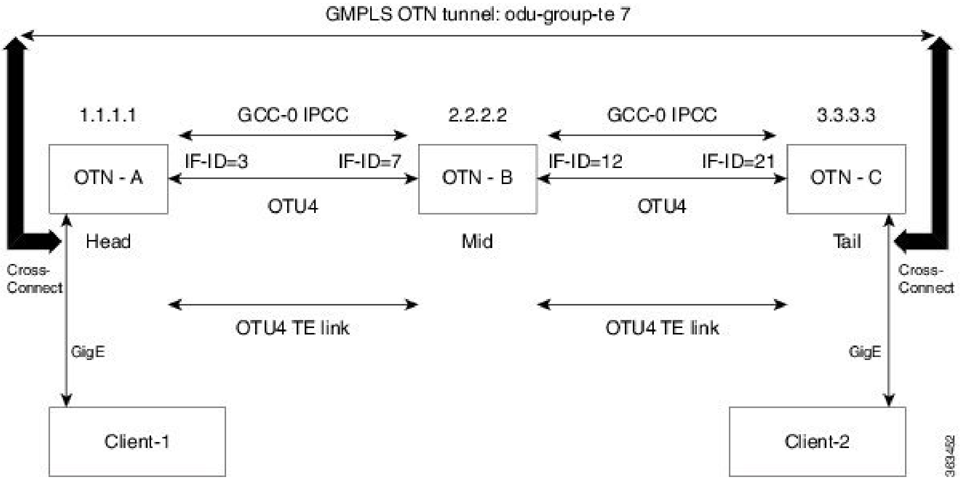
General Communication Channel (GCC) is an in-band side channel that carries transmission management and signaling information within optical transport network elements.

There are two types of GCC links:

- GCC0 - two bytes within OTUk overhead.
- GCC1 - two bytes within ODUk overhead.

Understand GMPLS

Generalized Multi-Protocol Label Switching (GMPLS) extends the packet based MPLS protocol to allow creation and maintenance of tunnels across the networks that consist of non-packet switching devices. GMPLS tunnels can traverse the Time-Division Multiplex (TDM) interface and switching types.



The following protocols are associated with GMPLS:

- **OSPF**
- **OSPF-TE**
- **RSVP-TE**
- **MPLS-TE**
- **LMP**

Understand Explicit Path

Explicit path refers to a user defined path taken by a circuit. GMPLS dynamically determines the path to be taken by a circuit but user can override this path by configuring an explicit path.

Interoperability between NCS 4000 and MSTP Nodes using NCS4K-4H-OPW-QC2 Card

Interoperability between NCS 4000 and MSTP nodes is achieved by creating a Link Management Protocol (LMP) numbered or unnumbered UNI link between NCS4K-4H-OPW-QC2 interface on the NCS 4000 node and the optical channel Add/Drop interface on the MSTP nodes.

To create OTN circuits between the NCS 4000 nodes via the MSTP network, a GMPLS OCH Trail circuit must be created between the two NCS 4000 nodes that are connected to MSTP nodes. The traffic transmitted by the OCH Trail circuit is used as a OTU4 or OTUC2 link by the OTN layer.

To configure interoperability, complete the Configure Interoperability Between NCS 4000 and MSTP Nodes, on page 99 procedure.

Provision Management IP Address

Purpose	This procedure provisions the manageme
Tools/Equipment	None
Prerequisite Procedures	" Login to CTC" in *System Setup and So*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, click the **Provisioning** > **Network** > **General** tabs.

Active RP—Displays the details of the active route processor.

Step 2 In the **Mgmt IP** area, complete the following information:

- Virtual IP Address - Enter an IP address drawn from the management IP address pool that supersedes the IP addresses of RP0 and RP1.
- Mask - Enter the subnet mask of the IP address.

Step 3 In the **RP0-EMS IP** and **RP1-EMS IP** areas, complete the following information:

- IPv4—Enter the IPv4 address assigned to RP0/RP1 EMS.
- IPv4 Mask—Enter the IPv4 subnet mask.
- Service State—Select the state from the drop-down menu. The available options are - IS (in-service) and OOS (out-of-service).

Step 4 In the **RP0-Craft IP** and **RP1-Craft IP** areas, complete the following information:

- IPv4—Enter the IPv4 address assigned to RP0/RP1 Craft panel.
- IPv4 Mask—Enter the IPv4 subnet mask.
- Service State—Select the state from the drop-down menu. The available options are - IS (in-service) and OOS (out-of-service).

Step 5 In the **RP0-Mgmt IP** and **RP1-Mgmt IP** area, complete the following information:

- IPv4—Enter an IP address drawn from the management IP address pool.
- IPv4 Mask—Enter the subnet mask for the IP address.
- Mac Address—Displays the MAC address of RP0/RP1.
- IPv6—Enter an IP address drawn from the management IP address pool.
- IPv6 Prefix Length—Enter the prefix length for the IP address.
- Service State—Select the state from the drop-down menu. The available options are - IS (in-service) and OOS (out-of-service).

Step 6 In the **Gateway** area, enter IPv4 or IPv6 address and enter the prefix length if you use IPv6 address. The prefix length must be between 0 and128.

Step 7 Click **Apply**.

Stop. You have completed this procedure.

Configure the Loopback on an Interface Using CTC

Purpose	This procedure provides instructions to configure the loopback on an interface using CTC. It also helps in management logging and authentication of a user on an interface for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS or NCS4K-4H-OPW-QC2 Line cards.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Maintenance** > **Loopback** tab.

Step 3 To configure loopback on OTN controllers, perform the following steps in the screen that appears:

a) Click the **Controller** column and select a name of the controller.
b) Click the **Admin State** Column.
c) Choose **Service State** for the controller. For more information, see Administrative and Service States, on page 11.
d) From the **Loopback Type** drop-down list, choose **Internal**, **Line** or **None**.
e) Click **Apply**.
f) Click **Refresh** to refresh all the controllers.

Stop. You have completed this procedure.

Enabling GMPLS Using CTC

Purpose	This procedure helps in enabling the Traffic Engineering (TE) links.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 To configure a GCC on a controller, complete Configuring GCC Using CTC, on page 74.

Step 2 To configure OSPF on an interface, complete Add OSPF on an Interface Using CTC, on page 75.

Step 3 To configure OSPF-TE, complete Configure OSPF-TE on an Interface Using CTC, on page 76.

Step 4 To configure MPLS-TE, complete Configure an MPLS-TE Instance Using CTC, on page 77.

Step 5 To configure RSVP-TE, complete Configure a RSVP-TE Instance Using CTC, on page 78.

Stop. You have completed this procedure.

Configuring GCC Using CTC

Purpose	This procedure enables you to configure General Communication Channel (GCC) on a controller for NCS4K-20T-O-S, NCS4K-2H-O-K, NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	Required.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double-click the line card.

Step 2 Click the **Provisioning** > **Controllers** > **OTU or ODU** tabs.

Step 3 To enable GCC on the controller, perform one of the following steps:

a) For OTU controller, check the **GCC0** check box.

b) For ODU controller, check the **GCC1** check box.

Step 4 Click **Apply**.

Step 5 In the Node View, click the **Provisioning** > **Comm Channels** tabs.

Step 6 To assign IP address to the GCC, add IP address in the **IP address** field and network mask in the **NetMask** field.

Note To assign loop back IP address to the GCC, select a **Loopback** from the drop down list.

Same loop back IP address can be assigned to multiple GCC's .

Step 7 Click **Apply**.

Step 8 Return to your originating procedure.

Add OSPF on an Interface Using CTC

Purpose	This procedure enables you to configure the OSPF on an interface using CTC. Adding OSPF allows to setup a link between two different routers and maintain the connectivity interface.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure the Loopback on an Interface Using CTC, on page 73
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **OSPF** tabs.

Step 2 Perform following steps to create an OSPF instance:

a) From **OSPF Instance Name** drop down list, select OTN.

b) From **Router Id** drop down list, select the router id.

Note Recommended configuration is Virtual IP.

c) Click **Apply**.

Step 3 Select the NSR check-box to enable redundant route processors to maintain its Open Shortest Path First (OSPF) state and adjacencies across planned and unplanned IP switchovers.

NSR stands for Non -Stop Routing.

Step 4 Select the NSF (IETF) check-box to continue forwarding IP packets following a supervisor engine switchover.

NSF stands for Non-Stop Forwarding.

Step 5 Perform following steps to add GCC interface to OSPF:

a) In **OSPF Interfaces** section, click **Add**. The Create OSPF Entry dialog box appears.

b) In the **Interface** drop down list, select the interface.

Note Add Loopback interface and GCC interface both, if loopback IP is assigned to GCC .

Repeat step3 to add multiple interfaces.

c) In the Area ID field, a default value of 0 is populated.(non-editable).

d) (Optional) In the Cost field, enter the cost.

e) (Optional) Check the **Passive** check box to ensure the updates are not sent beyond an OSPF interface.

f) Click **OK**.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure.

Configure OSPF-TE on an Interface Using CTC

Purpose	This procedure enables you to configure the OSPF-TE using CTC. OSPF-TE allows controlling the path of data packets and advertise the capabilities of TE links to remote nodes.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51 Add OSPF on an Interface Using CTC, on page 75
Required/As Needed	Required

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **OSPF-TE** tabs.

Step 2 From the **OSPF-TE Router Id** drop down list, select router id.

Note Recommended configuration is Virtual IP.

Step 3 To configure the OSPF-TE on an Interface, complete the following:

a) In the Area ID field, a default value of 0 is populated (non-editable).

b) Check the **Autoconfig** check box to enable all the interfaces of the OSPF-TE.

c) Click **Apply**.

Step 4 Return to your originating procedure.

Configure an MPLS-TE Instance Using CTC

Purpose	This enables you to configure an MPLS-TE instance that helps to route network traffic using CTC. Traffic engineering enables to reduce the cost of the network and offer the best service to the users.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC, on page 51
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **MPLS-TE** tabs.

Step 2 Click **Create**. The Create MPLS Topology Instance Entry dialog box appears.

Step 3 Click **OK** to create a MPLS-TE instance.

Step 4 In the **Controllers** section expand the row for the line card on which you want to configure MPLS-TE and perform the following steps to update the default values of the parameters:

a) To enable TE link, set **Enable** field as true.

b) From the **TTI mode** drop down list, select the TTI mode. Available options are PM, SM, TCM1,TCM2, TCM3, TCM4, TCM5, and TCM6.

c) (Optional) Set the **Admin Weight** field with value ranging from 0 to 65535.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure.

Configure a RSVP-TE Instance Using CTC

Purpose	This procedure enables you to configure a RSVP-TE instance.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As Needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **RSVP-TE** tabs.

Step 2 In the **Interface List** area, for an **Interface Name**, select the **RSVP State** from the drop-down menu. The available options are - Enable and Disable.

Step 3 In the **Card** section, expand the row for required LC to view the list of configured controllers.

Step 4 Select a controller and perform the following sub steps:

a) Set the **Enable** field of the controller to **true**.

b) (Optional) Input value for **Refresh Optical Interval**. Valid range is 180 to 86400 seconds.

c) (Optional) Input value for **Missed Messages**. Valid range is 1 to 110000.

Step 5 Click **Apply** to save the changes.

Stop. You have completed this procedure.

Configure OTN Circuits Using CTC

Purpose	This procedure configures an OTN Circuit Using CTC.
Tools/Equipment	None

Prerequisite Procedures	Configure an OTN Controller Using CTC, on page 51 Enabling GMPLS Using CTC, on page 74
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Perform any of the following procedures as needed to create, load, and store the path protection profile:

- Add a Path Protection Profile Using CTC, on page 79
- Load a Path Protection Profile Using CTC, on page 81
- Store a Path Protection Profile Using CTC, on page 82

Step 2 Perform any of the following procedures as needed to configure an OTN circuit:

- #unique_97
- Discover a Circuit Using CTC, on page 86
- Edit General Parameters of a Circuit Using CTC, on page 87
- Edit ODU Configuration of a Circuit Using CTC, on page 88

Step 3 Perform any of the following procedures as needed to create, load, and store the explicit path:

- Add an Explicit Path Using CTC, on page 91
- Store an Explicit Path Using CTC, on page 91
- Load an Explicit Path Using CTC, on page 92
- Create an LMP Using CTC, on page 93

Stop. You have completed this procedure.

Add a Path Protection Profile Using CTC

Purpose	This procedure provides instructions to add a path protection profile using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Path Protection Profiles**.

Step 2 Click **Add**. Perform the following steps in the editable row:

a) In the **Name** column, enter the Path Protection Profile name.

b) In the **Wait to Restore** (WTR) field (in seconds), enter the duration of time (in seconds).

> **Note** It defines the time the system must wait to restore a circuit. To edit the **WTR** value, **Revertive** should be set to **Yes**. The valid range is 0 or from 300 to 720 seconds. WTR value is in multiple of 60. Default value for WTR is 300.
>
> WTR is not supported on a non-revertive circuit.

c) From the **Sub Network Connection Mode** drop-down list, choose any from the following: SNC_N (default), SNC_I and SNC_S.

> **Note** A new entry will be created with Sub Network Connection Mode value as **SNC_N** and TCM-ID value as **NONE.**

d) In the **Hold Off (milli sec)** field, enter the duration of time (in seconds) .

> **Note** It defines the time the system waits before switching to the alternate path. The valid range is 0 or from 100 to 10000 seconds. Hold off value is in multiple of 100. Default value is 0.

e) From the **Protection Type** drop-down list, choose a protection type from the available options 1+1-BIDIR-APS (Default) or 1+1-UNIDIR-APS or 1+1-UNIDIR-NO-APS.

f) From the **Revertive** drop-down list, choose **Yes** or **No**. Default is **No**.

g) From the **TCM-ID** drop-down list, choose **None**.

Step 3 From the Sub Network Connection mode drop-down list, choose **SNC_S**.

Step 4 From the TCM drop-down list, choose an option.

> **Note** By default, **TCM-4** is selected once you select **SNC-S** as Sub Network Connection mode. You can change the TCM-ID column value from **TCM4** to TCM1-TCM6 for SNC-S.

> **Note** For SNC-I and SNC-N, You are not allowed to change the TCM-ID value. It should be set to **None**.

Step 5 Click **Store** to store the profile for the particular node.

Step 6 The Store Profile(s) window is displayed.

Step 7 By default, the **To Node(s)** radio button is selected. Select the required nodes from the **Node Names** area, to set the profile. Click **Select All** to set the profile for all the selected nodes. Click **Select None** to undo your earlier selection.

Step 8 Click **OK**.

Step 9 Select the **To File** radio button, and click **Browse** to save the profile in your local machine.

Step 10 Return to your originating procedure.

Provision Loopback Interface

Purpose	This procedure provisions the loopback interface

Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Softwa
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click the **Provisioning** > **Network** > **Loopback IF** tabs.

Step 2 If you want to create a loopback interface, complete the following:

- Click **Create**. The Create Loopback Interface dialog box appears.
- Enter the Interface ID, IP address, and network mask in the respective fields and click **OK**.

Step 3 If you want to edit a loopback interface, complete the following:

- Click **Edit**. The Edit Loopback Interface dialog box appears.
- Modify the values of the IP Address and network mask as required and click **OK**.

Step 4 Return to your originating procedure.

Load a Path Protection Profile Using CTC

Purpose	This procedure provides instructions to load a path protection profile using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning, higher or retriever

Procedure

Step 1 In the **Network View**, click the **OTN** > **Path Protection Profiles** tab.

Step 2 Click **Load**. Perform one of the following in the Load Profile (s) dialog box that appears.

a) From the **From Node (s)** pane, select a name of the node to load the path protection profiles.
b) Click **OK**.
c) In the **From File** field enter the path of the file or browse to the file, to load the path protection profile.

Note You can load the profiles from a file that has OTN extension.

d) Click **OK**.

Step 3 Return to your originating procedure.

Store a Path Protection Profile Using CTC

Purpose	Storing a Path Protection Profile allows to store cross connection on the same chassis. This procedure provides instructions to store a path protection profile using CTC.
Tools/Equipment	None
Prerequisite Procedures	• "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* • Add a Path Protection Profile Using CTC, on page 79 • Load a Path Protection Profile Using CTC, on page 81
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Path Protection Profiles**tab.

Step 2 Click **Store**. Perform one of the following in the Store Profile (s) dialog box that appears.

a) From the **To Node (s)** pane, select a name of the node to store the path protection profiles.

b) Click **Select All** to select all the node names.

c) Click **Select None** to deselect the selected node names.

d) To store the profile to a file, select the **To File** option and click**Browse** to select the required file, to store the path protection profile.

Step 3 Click **OK**

Step 4 Return to your originating procedure.

Configure an Open End OTN Circuit Using CTC

Purpose	OTN circuit allows the end user to setup end to end circuits from an origin to a destination Network Element. This procedure provides instructions to configure an open end OTN circuit using CTC.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Circuits** tab.

Step 2 Click **Create**. The Circuit Creation wizard appears.

Step 3 In the **Circuit Type** screen of the wizard, choose a circuit type **ODU UNI** from the list.

Step 4 Enter a value between 1 to 80 for the number of circuits to be created.

Step 5 Click **Next**.

Step 6 In the Circuit Attributes screen of the wizard:

a) From the **Source Node** drop-down list, choose a source node for the circuit.

b) From the **Destination Node** drop-down list, choose a destination node for the circuit.

c) In the **Name**field, enter the circuit name.

Note The length must not exceed 64 characters.

d) From the **Bandwidth** drop-down list, choose a bandwidth.

e) Click the **Bandwidth Configuration** hyperlink.

Note This hyperlink is enabled when you select the bandwidth type as **ODUFLEX**.

Perform the following steps in the Bandwidth Configuration dialog box that appears.

- In the **Bit Rate** field enter the bit rate. The bit rate per time slot is 1249177. Example for ODU2 we have 8 timeslots, so bit rate will be 1249177 * 8 = 9993416.
- From the **Framing Type** drop-down list, choose **CBR** or **GFP-F-Fixed** (for 10 Gigabit Ethernet).
- Click **OK**.

f) From the **Protection Type** drop-down list, choose an option **1+0**, **1+1** or **1+R**.

g) Click the **Path Option Configuration** hyperlink. The Path Option Configuration screen appears.

Note It is optional to configure the working path option. When you configure the path option using **Path Option Configuration** hyperlink, the selection made in the **Protection Type** drop-down list will be overridden.

Click **Add**. Perform the following steps in the Create/ Edit Path Option dialog box:

- In the **Index** field enter a unique index. The valid range is from 1 to 1000.
- In the **Path Option** drop-down list, choose **Working** or **Protect**.
- From the **Path Option Type** drop-down list, choose **Dynamic** or **Explicit**.

- From the **Path Name** drop-down list, choose an explicit path name.

  Note The **Path Name** field is disabled, if the path option type is dynamic.

- From the **Protected By** drop-down list, choose a protected path option.

  Note The **Protected By** drop-down list is disabled if the **Path Option** is set to Protect.

- From the **Restored By** drop-down list, select a restored path option. If any of the working or protected path fails, restored path replaces the failed path.

  Note The **Restored By** drop-down list is disabled if you have selected path option as Restored.

- Click **OK**.

h) From the **Path Protection Profile** drop-down list, choose an option. The option available is **None**. This drop-down list is disabled if protection type is selected as **1+0**.
i) Check the **Record Route** check box to record the route.
j) (For ODU UNI) From the **Service Type** drop-down list, select an option. Service type values are populated based on the bandwidth selected.
k) (For ODU UNI) Check the **Open End** check box to get the values populated in the Destination drop-down list.
l) (For ODU UNI) From the **Source drop-down list**, choose a source port or controller. Source values are populated based on the service type or open end selected
m) (For ODU UNI) From the **Destination** drop-down list, choose a destination port or controller. Destination values are populated based on the service type or open end selected..
n) Click the**Path Option Configuration hyperlink** button.

   Perform the following steps in the Create/Edit dialog box that appears.

   - From the ODU Level drop-down list, choose an option. ODU Level values are populated based on the Destination. ODU level is one less than the Destination. If Destination is selected as ODU2, values in this drop-down list would be ODU1 and ODU0.

   - Select a time slot highlighted in green color above, press Ctrl key and select the next time slot.

   - Click **Channelize** to allocate the time slot to the lower order channelize controller. The lower order controller appears in the controller tree hierarchy.

   - Click **OK**.

o) Click **Finish** to create the circuit.

Step 7 Return to your originating procedure.

Configure an OTN Circuit Using CTC

Purpose	This procedure configures an OTN circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	You can load the profiles from a file that has OTN extension.

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

Procedure

Step 1 In the network view, click the **OTN** > **Circuits** tab.

Step 2 Click **Create**. The Circuit Creation wizard appears.

Step 3 In the **Circuit Type** screen of the wizard, choose **ODU TUNNEL** as the circuit type.

Step 4 Click **Next**.

Step 5 In the Circuit Attributes screen of the wizard:

a) From the **Source Node** drop-down list, choose a source node for the circuit.

b) From the **Destination Node** drop-down list, choose a destination node for the circuit.

c) Enter the circuit name. The length must not exceed 64 characters.

d) Check the **Diversity** checkbox and choose the circuit from the drop-down list whose diverse circuit you want to create.

Note This step is applicable only when diverse circuit is created.

The drop down list will display <tunnel id>: <circuit name>

e) From the **Bandwidth** drop-down list, choose a bandwidth.

f) Click the **Bandwidth Configuration** hyperlink.

Note This hyperlink is enabled when you select the bandwidth type as **ODUFLEX**.

Perform the following steps in the Bandwidth Configuration dialog box that appears.

- In the **Bit Rate** field enter the bit rate.
- From the **Framing Type** drop-down list, choose **CBR** or **GFP-F-Fixed** (for 10 Gigabit Ethernet).
- Click **OK**.

g) From the **Protection Type** drop-down list, choose an option **1+0**, **1+1**, **1+R**,**1+1+R** .

Note Circuit diversity is supported only for 1+0 protection type.

h) Click the **Path Option Configuration** hyperlink. The Path Option Configuration screen appears.

Note This hyperlink is disabled when the **Diversity** checkbox is checked.

Click **Add**. Perform the following steps in the Create Path Option dialog box:

- In the **Index** field enter a unique index . The valid range is from 1 to 1000.
- From the **Path Option Type** drop-down list, choose **Dynamic** or **Explicit**.

Note For using the option Explicit, make sure that an explicit path is already defined. You can define an explicit path using procedure Add an Explicit Path Using CTC, on page 91.

- From the **Path Name** drop-down list, choose an explicit path name.

  Note The **Path Name** field is disabled, if the path option type is dynamic.

- From the **Affinity Attribute-Set Name** drop-down list, choose an affinity profile.
- From the **Protected By** drop-down list, choose a protected path option.

  Note The **Protected By** drop-down list is disabled for Restored or Protected path options.

- From the **Restored By** drop-down list, select a restored path option. If any of the working or protected path fails, restored path replaces the failed path.

  Note The **Restored By** drop-down list is disabled if you have selected path option as Restored.

- Click **OK**.

i) From the **Path Protection** Profile drop-down list, choose an option. The default option is **None**.

Note This drop-down list is disabled if protection type is selected as **1+0**.

j) Check the **Record Route** check box.

k) Click **Finish** to create the circuit.

Step 6 Return to your originating procedure.

Discover a Circuit Using CTC

Purpose	This procedure provides instructions to discover a circuits from the list of OTN circuits using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* #unique_97
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Circuits** tab.

Step 2 Click **Query**. Perform the following steps in the OTN Services Query screen that appears.

a) From the **Existing/New Query** drop-down list, choose **New** or **Existing**.

b) Enter the tunnel IDs if you have selected **New Query**.

Note For **Existing Query**, Tunnel IDs and Query Group fields are populated automatically.

c) Click **Query Group**. Perform the following steps in the User Query Group Chooser dialog box:

- From the **Group** drop-down list, choose an option.
- From the **Available Nodes** pane, choose a node.
- Click >> to move the selected node from the Available Nodes to the Grouped Nodes pane.
- Click **Save** to save this query group criteria. A dialog box appears, enter a name for the query group and click **Save**.
- Click **Apply All** to select all the available nodes. These nodes appear in the field next to the **Query Group** button.
- Click **Apply Selected** to select only the grouped nodes. These nodes appear in the field next to the **Query Group** button.

d) Click **Save** to save the query criteria.

e) Click **Run Query** to execute the query.

Note The **Run Query** button gets enabled only when you enter a value in the Query Group field. The search result appears in the Query Matches pane.

f) Enter a search criteria in the field adjacent to the **Find Next** button.

Note This button gets enabled only when you have a value in the Query Matches pane.

g) Click **Find Next**.

Note The next value gets highlighted in the Query Matches pane based on the search criteria.

h) From the **Query Matches** pane, choose a **circuit**.

i) Click >> to move the selected circuit from the **Query Matches** pane to the **Selected Services** to Discover pane.

j) Click **Discover All** to display all the circuits of the **Query Matches** pane on the **Circuits** tab.

k) Click **Discover Selected** to display all the selected circuit of the Selected Services to Discover pane on the **Circuits** tab.

Step 3 Return to your originating procedure.

Edit General Parameters of a Circuit Using CTC

Purpose	This procedure provides instructions to edit general parameters of an OTN circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Network View, click the **OTN** > **Circuits** tabs.

Step 2 Select a circuit and click **Edit**.

Step 3 Click the **General** tab. Perform the following steps in the Edit Circuit screen that appears:

a) Modify the parameters such as **Name**, **Bandwidth**, **Path Protection Profile**, **Bandwidth Configuration**, **Diversity** and **Source and Destination** client interfaces as needed.

Note Details of source and destination client interfaces are editable only when you update UNI circuits.

Note The **Path Option Configuration** hyperlink is disabled when the **Diversity** checkbox is checked or when diverse circuit of the selected circuit exists.

b) Click **Apply** to save the changes.

Note CTC hangs for a minute when multiple edit circuit windows are opened with multiple pluggable OIR.

Step 4 Return to your originating procedure.

Edit ODU Configuration of a Circuit Using CTC

Purpose	This procedure helps to edit the ODU configuration of a circuit.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* #unique_97 Discover a Circuit Using CTC, on page 86
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Circuits** tab.

Step 2 Select a circuit from the list.

Step 3 Click **Edit**.

For the procedure to view TCM parameters, see View TCM PM Parameters Using CTC, on page 121

Step 4 Click **ODU Configuration** tab.

Step 5 From the left pane, click the **ODU Line Configuration** tab. Perform the following steps in the Edit ODU Line Configuration screen that appears:

a) Select a controller from the list.
b) From the **Admin State** drop-down list, choose **Automatic in Service**, **Maintenance** or **Normal**.

Note This field displays the current status of a controller.

c) From the **Loopback** drop-down list, choose an option **Internal**, **Line** or **None**.
d) From the **GCC1** drop-down list, choose **Enable** or **Disable**.
e) Click **Apply**.

Step 6 From the left pane, click the **ODU TTI Configuration** tab. Perform the following steps in the Edit ODU TTI Configuration screen that appears:

Note TTI configuration is not supported on HO ODUs.

a) From the **Controller Name** drop-down list, choose controllers for the **Source** and **Destination** pane respectively.

Note The values that you enter in the **Transmit** area of the **Source** pane are displayed in the corresponding fields of the **Expected** area of the **Destination** pane. Similarly, the values that you enter in the **Expected** area of the **Source** pane are displayed in the corresponding fields of the **Transmit** area of the **Destination** pane. The values of the **Received** area of the **Source** and **Destination** pane must be the same.

b) In the **Transmit** area, click **ASCII** or **Hex (1 byte)** to specify the data type for the operator string.
c) Click **ASCII Mode**. The operator string is converted to ASCII data type.
d) Enter a new operator string. This string replaces the operator specific string when you click **Apply**.
e) Repeat steps (b) through (d) to select a data type in the **Expected** area of the **Source** pane.
f) Check the **Auto-Refresh** check box to refresh the received operator specific value automatically in every 5 seconds.
g) Click **Apply**.

Step 7 From the left pane, click the **TCM Line Configuration** tab. Perform the following steps in the Edit TCM Line Configuration screen that appears:

a) From the **Controller Name** drop-down list, choose a node.
b) From the **TCM Mode** drop-down list, choose a mode.

The available options are:

- Transparent - TCM data is passed through without any change , fault management and performance monitoring parameters are not enabled.
- Operational - fault management (the LTC-CA alarm can be enabled) and performance monitoring parameters can be enabled.
- NIM (Non-Intrusive Monitoring) - Performance monitoring parameters are enabled but are read-only. The LTC-CA alarm cannot be enabled.

c) Check the **Enable PM** check box to enable performance monitoring. This check box can be selected when the TCM Mode is either Operational or NIM.

d) Select the **LTC-CA** (Loss of Tandem Connection-Consecutive Action) check box to enable this alarm. This check box can be selected only when the TCM Mode is Operational.

e) Select the **TIM-CA** (Trace Identifier Mismatch-Consecutive Action) check box to enable this alarm. This check box can be selected only when the TCM Mode is Operational.

f) Click **Apply**.

Step 8 From the left pane, click the **TCM TTI Configuration** tab. Perform the following steps in the Edit TCM TTI Configuration screen:

a) From the **Controller Name** drop-down list, choose controller for the **Source** and **Destination** pane respectively.

Note The values that you enter in the **Transmit** area of the **Source** pane are displayed in the corresponding fields of the **Expected** area of the **Destination** pane. Similarly, the values that you enter in the **Expected** area of the **Source** pane are displayed in the corresponding fields of the **Transmit** area of the **Destination** pane. The values of the **Received** area of the **Source** and **Destination** pane must be the same.

b) From the TCM drop-down list, choose TCM on the **Source** and **Destination** pane respectively.

c) In the **Transmit** area, click **ASCII** or **Hex (1 byte)** to specify the data type for the operator string.

d) Click **Hex Mode**. The operator string is converted to hexadecimal data type.

e) Enter a new operator string.

f) Click **Apply** to replace the operator specific string.

g) Repeat steps (c) through (e) to select a data type in the **Expected** area of the **Source** pane.

h) Select the **Auto-Refresh** check box to refresh the received operator specific value automatically, every 5 seconds.

i) Click **Apply**.

Step 9 From the left pane, click the **PM Thresholds** tab.

a) Click the **ODU Controller** tab. Perform the following steps in the ODU controller screen that appears:

Note Performance monitoring should be enabled for ODU controllers.

- From the **Controller Name** drop-down list, choose a **controller**.
- From the **Layer Name** drop-down list, choose an option **Path** or **GFP**. The PM threshold values get populated in the table appears on the screen.
- Click either **15 Min** or **1 Day** interval to get the PM interval.
- Click **Refresh** to get the updated PM threshold values in the table from the legacy node.

b) Click the **TCM** tab. Perform the following steps in the TCM screen that appears:

Note Permon should be enabled for TCM controllers.

- From the **Controller Name** drop-down list, choose a controller. The PM threshold values get populated in the table appears on the screen.
- Click either **15 Min** or **1 Day** interval to get the PM thresholds interval.
- Click **Refresh** to get the updated TCM PM threshold values from the legacy node.

Step 10 Return to your originating procedure.

Add an Explicit Path Using CTC

Purpose	This procedure provides instructions to create an explicit path using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* Configure OTU for OTN Controller Using CTC, on page 53
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Explicit Paths**.

Step 2 Click **Add**. Perform the following steps in the Create Explicit Path screen:

a) Enter a name of the explicit path.

Note Strict path type is selected by default.

b) Click **Add**. Perform the following steps in the Add Node dialog box. Alternately, select a node from the map, and click **Add**.

- From the **Node** drop-down list, choose**node**.
- From the **Interface** drop-down list, choose an **interface**.
- Click **Apply**.

c) Click **Apply** to save the explicit path.

Step 3 Return to your originating procedure.

Store an Explicit Path Using CTC

Purpose	This procedure provides instructions to store an explicit path using CTC.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* Add an Explicit Path Using CTC, on page 91
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **Explicit Paths** > **Explicit Paths** tab.

Step 2 Click **Store**. Perform the following steps in the Store Explicit Path (s) dialog box:

a) Check the check box adjacent to a node name.

b) Click **OK** to store the explicit path.

Step 3 Return to your originating procedure.

Load an Explicit Path Using CTC

Purpose	This procedure provides instructions to load an explicit path using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* Store an Explicit Path Using CTC, on page 91
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Explicit Path**.

Step 2 Click **Load**. Perform the following steps in the Load Explicit Path (s) dialog box:

a) Check the check box adjacent to a node name.

b) Click **OK** to load the explicit path.

Step 3 Return to your originating procedure.

Create an LMP Using CTC

Purpose	Link Management Protocol (LMP) is used to manage Traffic Engineering (TE) links. It allows multiple data links into a single Traffic Engineering (TE) link that runs between a pair of nodes. Link Management Protocol (LMP) is used to support interoperability between the NCS 4000 node and the MSTP node. The LMP creation wizard allows you to provision the source and destination end-points of the LMP link, the optical parameters, and alien wavelength settings.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **Provisioning** > **LMP** tabs.

Step 2 Click **Create**.

The LMP Creation wizard appears.

Step 3 In the LMP Origination screen of the wizard, provision these parameters.

- From the **Originating Node** drop-down list, choose the source node of the LMP.

  Note If the source node is NCS 4000, then the destination node must be MSTP.

- Click **Unnumbered** if you want to create an unnumbered LMP.

  Note The Interface IP field is disabled.

- In the Communication Channel field ,enter the router IP address.
- From the **Mode** drop-down list, choose UNI for an unnumbered optical UNI.
- From the **Local Interfaces** drop-down list, select the port that is connected to the DWDM node.
- Enter the IP address of the source node in the Interface IP field. This field is enabled only if the Numbered option was selected.

Step 4 Click **Next**.

Step 5 In the LMP Termination screen of the wizard, provision these parameters:

- From the **Terminating Node** drop-down list, choose the destination node of the LMP.
- Rx Port Selection—Choose the card type from the Type drop-down list; choose a unit from the Unit drop-down list; choose a port from the Port drop-down list.

- Tx Port Selection—Choose the card type from the Type drop-down list; choose a unit from the Unit drop-down list; choose a port from the Port drop-down list.
- Enter the IP address of the destination node in the Interface IP field.

  Note The Interface IP field is disabled if the Unnumbered option was selected in the LMP Origination screen of the wizard.

- Mode—Sets the type of revertive restoration to either UNI-C or UNI-N. If the mode is set to UNI-C, the reversion of the circuit from the restored path to the original path is triggered by the UNI client. If the mode is set to UNI-N, the reversion of the circuit is triggered by the DWDM network and can be either a manual revert or an auto revert.

Step 6 Click **Next**. Perform the following steps in the Optical Parameters screen that appears in the LMP creation wizard:

Step 7 In the Optical Parameters screen of the wizard, provision these parameters:

- Check the **Allow Regeneration** check box (optional).

  Note When checked, the computed path traverses through the regeneration site only if optical validation is not satisfied. If a transparent path is feasible, the regenerator is not used.

- From the **UNI State** drop-down list, choose **Enable** or **Disable**.

  Note The Enable state is used to configure the UNI interface for the circuits to pass through, between the router and DWDM node. In the Disable state, the interface is configured but not active and circuit activation is rejected. When the status is changed from Enable to Disable, all the active circuits on the interface are deleted.

- Description—Enter the description of the UNI interface. The description can be up to 256 characters.
- Label—Enter an alphanumeric string. This label is an unique circuit identifier.
- Validation—Sets the optical validation mode.
- Acceptance threshold—Sets the acceptance threshold value for the GMPLS circuit. The circuit is created if the actual acceptance threshold value is greater than, or equal to, the value set in this field.
- Restoration—Check this check box to enable the restoration of the GMPLS circuits on the UNI interface.
- Validation—Sets the validation mode during restoration.
- Acceptance threshold—Sets the acceptance threshold value for the GMPLS circuit. The circuit is restored if the actual acceptance threshold value is greater than, or equal to, the value set in this field.

Step 8 Click **Next**.

Step 9 In the Alien Wavelength screen of the wizard, provision these parameters:

- From the **Alien Wavelength** drop-down list, choose an alien wavelength class.

  Note Choose the 400G-XP-LC-CFP2 wavelength if the NCS4K-4H-OPW-QC2 card is used for creating the LMP between the NCS 4000 and MSTP nodes.

- From the Trunk Selection drop-down list, choose 100G or 200G

  Note Choose 100G or 200G if the port is provisioned as OTU4 or OTUC2 respectively.

- From the **FEC** drop-down list, choose the forward error correction (FEC) mode on the alien wavelength channel. The following options are available:
    - 15% Soft Decision FEC DE OFF
    - 25% Soft Decision FEC DE OFF
    - 15% Soft Decision FEC DE ON
    - 25% Soft Decision FEC DE ON

  Note Choose the FEC configuration that matches the one in use on the NCS4K-4H-OPW-QC2 CFP2 interface.

Note This step is applicable when an LMP is created between NCS 4000 and MSTP nodes.

Step 10 Click **Finish** to create the LMP.

Step 11 Return to your originating procedure.

Create a Permanent Connection Using CTC

Purpose	This procedure enables you to create a permanent connection for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC. Permanent connection allows to create a cross-connection.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node/Card View, double-click the line card.

Step 2 Click the **Circuits** > **Permanent Connection** tab.

Step 3 Click **Create**. Perform the following steps in the Create Permanent Connection dialog box that appears.

Note User is allowed to create high order cross connection only. The high order being used should not be channelized. All the permanent connections (except high order connections) are read only.

a) Enter the **XConnect Name** of the permanent connection. The connection ID value ranges from 1 to 32655.
b) From the **End Point 1** drop-down list, select the ingress point of the permanent connection.
c) From the **End Point 2** drop-down list, select the egress point of the permanent connection.

d) Click **OK**.

Stop. You have completed this procedure.

Perform a Path Switch

Purpose	This procedure enables you to perform a path switch. The possible actions are: • Manual Switch Over • Force Switch Over • Lockout (available only on a working circuit)
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View** , click the **OTN > Circuits** tab.

Step 2 Select a circuit from the list. Ensure that the **Type** is 1+1.

Step 3 Click **Edit**.

Step 4 Click the **Protection** tab.

Step 5 The details of the selected circuit are displayed under the Source and Destination . The working circuit details are in green and the protect circuit details are in purple.

The same details are represented in a pictorial format, in the **File** section. To perform the switchovers, use this pictorial format.

Step 6 Right-click the port of the working circuit or the protect circuit.

The available options are:

- Open Port - opens the card view of the line card.
- Switch commands - displays the available switch over options.

Step 7 Select one of the options under Switch commands.

The available options are:

- Manual Switchover - to switch from the working to the protect circuit or vice-versa

- Force Switchover - to switch back to the working circuit
- Exercise - to check the protocol in use
- Lockout (available only for a working circuit)- the path continues to be on the working circuit (even if a failure is detected on the working circuit)
- Clear Lockout (available only for a working circuit)- the path can now use the protect circuit
- Clear - clears the manual switch option (not available when the path is in the lockout mode)

Step 8 Return to the originating procedure.

Configuring OTN Circuits Using Node Configuration Wizard

Purpose	This procedure configures the OTN circuits using Node Configuration Wizard.
Tools/Equipment	None
Prerequisite Procedures	
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View** or **Card View**, right-click anywhere and choose the **Node Configuration Wizard**

Step 2 In the **IP Configuration** pane, if you want to provision the Virtual IP, Management IP, EMS IP, Craft IP, Gateway IP and the corresponding mask, complete the following :

a) Enter the **Virtual IP Address** drawn from the management IP address pools that supersede the IP address of RP0 and RP1.

b) Enter the **Subnet Mask** for the Virtual IP address previously entered.

c) In the **RP0-Mgmt IP** and **RP1-Mgmt IP** areas, complete the following information:

- IPv4—Enter a unique IPv4 address assigned to RP0/RP1. It displays blank if not configured.
- IPv4 Mask—Enter the IPv4 subnet mask.
- Rp0 or Rp1 Service State - Select an option from the drop-down menu. The available options are IS, OOS.
- MAC Address—Displays the MAC address of RP0/RP1.
- IPv6 —Enter the IPv6 address assigned to RP0/RP1.
- IPv6 Prefix Length—Enter the prefix length for the provisioned IPv6 address. The value must be between 1 and 128.
- EMS Interface --- Displays the IP address of RP0/RP1 that connects to a device via serial or LAN port.

- EMS Submask --- Displays the subnet mask corresponding to the EMS IP.
- EMS Service State - Select an option from the drop-down menu. The available options are IS, OOS.
- Craft Interface --- Displays the IP address of RP0/RP1 that connects to a device via serial or LAN port.
- Craft Submask --- Displays the subnet mask corresponding to the Craft IP.
- Craft Service State --- Select an option from the drop-down menu. The available options are IS,OOS.

Note If your node is having dual RP, then you must configure both the RP0 and RP1 to avoid discrepancy while performing switchover.

d) In the Gateway area, complete the following information :

- IPv4 --- Enter a unique IPv4 address.
- IPv6 --- Enter a unique IPv6 address.
- IPv6 Prefix Length --- Enter the prefix length for the provisioned IPv6 address. The value must be between 1 and 128.

Step 3 Click the **Next** button to save the changes and open the **OTN Topology** pane.

Step 4 Click **Close** to save the changes and close the Node Configuration Wizard.

Step 5 In the loopback interface area, complete the following :

- Interface Type/ID --- Displays the loopback0 and it cannot be modified.
- IP Address --- Configure the Loopback IP Address.
- Sub Net Mask -- Enter the Subnet Mask for the Loopback IP Address.

You cannot delete the Loopback information once configured.

Step 6 In the RSVP-Interface List area, the details include:

- Interface Name - displays the interface.
- RSVP State - choose an option from the drop-down menu. The available options are - Disable and Enable.

Step 7 If you want to create the controller, configure GCC interface, MPLS-TE, RSVP-TE on a particular card, complete the following :

a) In the Port Controller Configuration area, click the **Slot** to see the already configured ports with its corresponding data. The ports which are not configured on the node display the value None.

b) Displays the **Port** number.

c) Displays the **Service State** for the port. The states can be --- IS-NR, OOS-AU.

d) Select a **Service Type** from the drop-down list to create the controller.

e) Check the **GCC0/GCC1** check box if you want to enable GCC on OTU or ODU in each slot.

f) Check the **Unnumbered GCC0/1** check box to assign unnumbered loopback only on the enabled GCC interfaces.

g) Check the **MPLS** check box if you want to configure the specific controller as a part of MPLS configuration. Complete Configure an MPLS-TE Instance Using CTC, on page 77 as needed.

h) Check the **RSVP** check box if you want to configure the specific controller as a part of RSVP configuration. Complete Configure a RSVP-TE Instance Using CTC, on page 78 as needed.

i) Configure the value of **Admin weight** only if MPLS is enabled. This weight ranges from 0 to 65535.

The default value of Admin weight is 0.

j) Configure the value of **TTI Mode** only if MPLS is enabled.

k) Configure the value of **Timer** only if RSVP is enabled. It ranges from 180 to 86400 seconds.

l) Configure the value of **Missed messages** field only if RSVP is enabled. It displays the number of refresh optical missed messages and ranges from 1 to 8.

Step 8 If you want to delete the controller, perform the following:

a) Click the **Next** button to save the current changes and open the **OTN Topology** pane.

b) Choose the **Service Type** as **None** to delete the already configured controller.

c) Click the **Previous** button to save the changes and display the previous configuration pane.

d) Click the **Close** button to save the changes and close the Node Configuration Wizard.

Delete the controller manually from the MPLS or RSVP, If you have configured the controller as part of MPLS or RSVP configuration.

Step 9 In the **OSPF** area, Complete the following :

- OSPF Process ID --- Displays OTN and cannot be modified.
- Router ID --- Displays the virtual IP of the node.
- Enable NSR --- Displays the field as checked once the OSPF process ID and Router ID is created.
- Enable NSF --- Displays the field as checked once the OSPF process ID and Router ID is created
- Add --- Click this button to create an OSPF entry.
- Delete --- Click this button to delete a selected OSPF entry.
- Interface --- Choose the OSPF interface from the drop-down list.
- Area ID --- Displays area ID as 0.
- Cost --- Enter the cost used by OSPF routers to calculate the shortest path.
- Passive --- Choose the state of the OSPF interface from the drop-down list. The available options are True and False.

Step 10 Click **Previous** to save the current changes and display the previous configuration pane.

Step 11 Click **Close** to save the changes and close the Node Configuration Wizard.

Stop. You have completed this procedure.

Configure Interoperability Between NCS 4000 and MSTP Nodes

Purpose	Link Management Protocol (LMP) is used to support interoperability between the NCS 4000 node and the MSTP node. To support interoperability, this procedure provisions an LMP between an NCS 4000 node and MSTP nodes followed by the creation of an GMPLS OCH trail circuit between two NCS 4000 nodes.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 To provision an LMP between an NCS 4000 and MSTP node, complete Create an LMP Using CTC, on page 93.

Step 2 To provision a TE link, complete Enabling GMPLS Using CTC, on page 74.

Step 3 To provision a GMPLS OCH trail circuit between two NCS 4000 nodes, complete Configure GMPLS OCH Trail Between NCS 4000 Nodes, on page 100

Stop. You have completed this procedure.

Configure GMPLS OCH Trail Between NCS 4000 Nodes

Purpose	This task provisions a GMPLS OCH trail circuit between NCS 4000 nodes that are connected to MSTP nodes.
Tools/Equipment	None
Prerequisite Procedures	• "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* • Create an LMP Using CTC, on page 93
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the network view, click the **DWDM Functional View** icon in the toolbar. The DWDM Network Functional View <Circuit Maintenance> opens.

Alternatively, you could perform the following steps in the network view:

- Click **Circuits** > **Circuits** tabs.
- Click **Create**. The Create Circuit dialog appears.
- Click **WSON**. The DWDM Network Functional View <Circuit Maintenance> opens.

Step 2 From the Change Perspective drop-down list in the toolbar, choose **Circuit Creation**. The Circuit Creation view opens.

Step 3 Select the source node from where the OCH trail circuit must originate.

Step 4 Right-click and select the originating port on the source node.

Step 5 Select the destination node where the OCH trail circuit must terminate.

Step 6 Right-click and select the terminating port on the destination node.

The GMPLS/WSON OCH_TRAIL Selection window appears.

Step 7 Specify a name and label for the circuit.

Step 8 Set the validation mode and acceptance threshold.

Step 9 Check the Wavelength Configuration check box to configure an explicit wavelength for the circuit.

Step 10 Check the IS checkbox to place the OCH trail circuit in service after creation. It is checked by default.

Step 11 Click **Create**.

All the configurations are applied to the circuit. The circuit appears in the Circuits tab in the Network Data pane.

Step 12 Return to your originating procedure.

CHAPTER 7

Configure the Bridge and Roll

Bridge allows data to setup a link to another path when original path requires any maintenance. After the maintenance of the original path, Roll allows to revert the path. This chapter provides the CTC procedures to configure the bridge and roll.

- Configure Bridge and Roll Using CTC, on page 103

Configure Bridge and Roll Using CTC

Purpose	Bridge allows setup a link between two temporary paths when the main path requires any maintenance. Rolls allows to get revert the temporary path once maintenance done of the main path. This chapter provides the CTC procedures to configure the bridge and roll.
Tools/Equipment	None
Prerequisite Procedures	#unique_97
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed to configure the bridge and roll:

- Add an Explicit Path to an unprotected OTN Circuit for a Roll Over Using CTC, on page 104
- Perform a Manual Switch Using CTC, on page 104

Stop. You have completed this procedure.

Add an Explicit Path to an unprotected OTN Circuit for a Roll Over Using CTC

Purpose	This procedure enables you to add an explicit path to an unprotected OTN circuit for a roll over for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC. Adding an Explicit Path allows to roll over into the original path.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* #unique_97
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Onsite/Remote	Provisioning or higher

Procedure

Step 1 In the Network View, double-click the line card.

Step 2 Click the **OTN** > **Circuit** tab.

Step 3 Select a circuit from the list.

Step 4 From the **Tools** menu, choose **Circuit**.

Step 5 Click **Roll Circuit**. Perform the following steps in the Select a Member Circuit to Roll screen that appears.

Note The roll, a circuit feature is not from the node perspective but from the CTC session perspective. If the session is closed in between, information about rolls cannot be recovered.

a) From the Explicit Path drop-down list, choose an explicit path that you want to add to the selected circuit.
b) Click **Add** to add the selected explicit path to the circuit

Step 6 Return to your originating procedure.

Perform a Manual Switch Using CTC

Purpose	This procedure enables you to perform a manual switch for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC. Manual Switch allows the traffic to switch from the working path to the protected path.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*

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

Procedure

Step 1 In the Network View, double-click the line card.

Step 2 Click the **OTN** > **Rolls** tab.

Step 3 Select a circuit from the list.

Step 4 Click **Manual Switch Over**.

The traffic is switched from the working path to the protected path.

Step 5 Return to your originating procedure.

CHAPTER 8

Configure Performance Monitoring

This chapter describes the CTC procedures to configure the performance monitoring for various controllers. Performance Monitoring provides a generic mechanism to collect historical and current values .

Understand Performance Monitoring

- Performance Monitoring (PM) helps service providers to gather performance counter for the system maintenance and troubleshooting. User can retrieve both the current and the historical PM counters.
- User can collect current 15 minutes and 1 day interval PM counter values for the various controllers. In 15 minutes interval, user can collect 33 buckets (one current bucket and 32 historical buckets) for PM counter values.
- Each bucket maintains 15 minutes interval PM accumulative counter values. However, for 1 day interval, user can collect two buckets for PM counter values. First bucket shows the latest 24 hour PM counter values and second bucket shows the previous day PM counter values. These PM counter values can be retrieved for the far end and the near end nodes

Procedure to displays the PM parameters of a controller can be performed using following Cisco IOS XR commands:

Understand Threshold Crossing Alerts (TCA)

Thresholds set the acceptable error levels for each PM attribute, when this level is violated TCA shall be reported for respective PM bins.

Every Threshold Crossing Alarms (TCA) that gets generated by the network element must be sent to corresponding the Network Management system (NMS).

Configure Performance Monitoring Using CTC

Purpose	This chapter describes the procedures to configures the performance monitoring.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Perform any of the following procedures as needed to view the PM parameters of a controller.

Note To enable or disable a particular TCA on a controller, you need to select each and every controller specifically. To enable or disable TCA on all the controllers, use command line interface.

- Edit Performance Monitoring Parameters Using CTC, on page 109
- View Optics PM Parameters Using CTC, on page 110
- View Optical Carrier (OC) PM Parameters Using CTC, on page 111
- View Synchronous Transport Signal (STS) PM Parameters Using CTC, on page 112
- View Synchronous Transport Module (STM) PM Parameters Using CTC, on page 113
- View Virtual Concatenation (VC) PM Parameters Using CTC, on page 114
- View Ethernet PM Parameters Using CTC, on page 115
- View OTU PM Parameters Using CTC, on page 118
- View FEC PM Parameters Using CTC, on page 119
- View ODU PM Parameters Using CTC, on page 120
- View TCM PM Parameters Using CTC, on page 121

Step 2 Perform any of the following procedures as needed to change the PM display:

- View PM Counts at 15-Minute/1Day Intervals Using CTC, on page 122
- View Near-End/Far-End PM Counts Using CTC, on page 123
- Reset Current PM Counts Using CTC, on page 124
- Clear Selected PM Counts Using CTC, on page 125
- Set the Auto-Refresh Interval for Displayed PM Counts Using CTC, on page 126

Step 3 Perform any of the following procedures as needed to change the PM threshold:

- Set the PM Threshold Values Using CTC, on page 127
- Reset PM Thresholds Using CTC, on page 128
- Refresh PM Threshold at 15-Minute/ 1Day Intervals Using CTC, on page 128

Stop. You have completed this procedure.

Edit Performance Monitoring Parameters Using CTC

Purpose	This procedure provides instructions to edit performance monitoring parameters of an OTN circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* #unique_97
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click a **line card**. The **Card View** appears.

Step 2 Click the **Circuits** > **OTN Circuits** tab. A list of OTN circuits appear.

Step 3 Select a circuit from the table.

Step 4 Click **Edit**.

Step 5 Click the **Performance Monitoring** > **ODU Controller** tab.

a) Click the **Current Values/Historical** tab. PM values from the legacy node appear on the table for the default controller. To update this populated table, perform the following steps on the Current Values tab that appears:

- From the **Controller Name** drop-down list, choose a **controller**. The PM values in the table gets updated accordingly.
- From the **Layer Name** drop-down list, choose an option **Path** or **GFP**.

  Note The PM values in the table gets updated accordingly.

- Click either **Near End** or **Far End** direction to get the PM direction.
- Click either **15 Min** or **1 Day** interval to get the PM interval.

  Note The PM values in the table gets updated accordingly.

- Click **Refresh** to get the current ODU Controller PM values.
- From the **Auto-Refresh** drop-down list, choose an **option** to refresh the current PM values at the selected interval automatically.

Step 6 From the left pane, click the **TCM**.

a) Click the **Current Values** tab. PM values from the legacy node appear on the table for the default controller. To update this populated table, perform the following steps on the current values tab that appears:

Note Click **Clear** to clear the value

Note The difference between **Threshold** and **Current counters** will appear by selecting Baseline.

- From the **Controller Name** drop-down list, choose a controller. The PM values in the table gets updated accordingly.
- Click either **Near End** or **Far End** direction to get the PM direction.

  Note The PM values in the table gets updated accordingly.

- Click **Refresh** to get the current TCM PM values from the legacy node.
- From the **Auto-Refresh** drop-down list, choose an option to refresh the current PM values at the selected interval automatically.

b) Click the **Historical** tab. PM values from the legacy node appear on the table for the default controller. To update this populated table, perform the following steps on the historical values tab that appears:

- From the **Controller Name** drop-down list, choose a **controller**. The PM values in the table gets updated accordingly.
- From the **TCM** drop-down list, choose a TCM. The PM values in the table gets updated accordingly.
- Click either **Near End** or **Far End** direction to get the PM direction.

  Note The PM values in the table gets updated accordingly.

- Click either **15 Min** or **1 Day** interval to get the PM interval.

  Note The PM values in the table gets updated accordingly.

- Click **Refresh** to get the historical TCM PM values from the legacy node.
- From the **Auto-Refresh** drop-down list, choose an **option** to refresh the historical PM values at the selected interval automatically.

Step 7 Return to your originating procedure.

View Optics PM Parameters Using CTC

Purpose	This procedure displays the optics PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **Optics** > **Current Values** tab.

Step 3 Click the **Historical** tab to view the PM parameter names that appear in the Parameter column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 5: Optics PM parameters

Optics PM Parameters	Definition
Laser Bias %	Displays the laser bias percentage.
Tx Optical Power (dBm)	Displays the transmit power level.
Rx Optical Power (dBm)	Displays the receive power level.

Step 4 Return to your originating procedure.

View Optical Carrier (OC) PM Parameters Using CTC

Purpose	This procedure displays the Optical Carrier (OC) PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node view**, double-click the line card.

Step 2 Click the **Performance** > **SONET** > **OC Current Values**tab to view the current PM parameter names and values.

Step 3 Click the **OC Historical** tab to view the PM parameter names and values that appear in the **Parameter** column.

.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 6: OC PM Parameters

OC PM Parameters	Definition
CV-S	Displays the number of section coding violations on the node.
ES-S	Displays the number of section error seconds on the node.
SEFS-S	Displays the number of section severely error framing seconds on the node.
SES-S	Displays the number of section severely error seconds on the node.
CV-L	Displays the number of line coding violations on the node.
ES-L	Displays the number of line error seconds on the node.
FC-L	Displays the number of line failure counts on the node.
SES-L	Displays the number of line severely error seconds on the node.
UAS-L	Displays the number of line unavailable seconds on the node.

Step 4 Return to your originating procedure.

View Synchronous Transport Signal (STS) PM Parameters Using CTC

Purpose	This procedure displays the Synchronous Transport Signal (STS) PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **SONET** > **STS Current Values** tab to view the current PM parameter names.

Step 3 Click the **STS Historical** tab to view the PM parameter names that appear in the **Parameter** column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 7: STS PM Parameters

STS PM Parameters	Definition
CV-P	Displays the number of path monitor coding violations on the node.
ES-P	Displays the number of path monitor errored seconds on the node.
SES-P	Displays the number of path monitor severely errored seconds on the node.
UAS-P	Displays the number of path monitor unavailable seconds on the node.

Step 4 Return to your originating procedure.

View Synchronous Transport Module (STM) PM Parameters Using CTC

Purpose	This procedure displays the Synchronous Transport Module (TM) PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **SDH** > **STM Current Values** tab to view the current PM parameter names.

Step 3 Click the **STM Historical** tab to view the PM parameter names that appear in the Parameter column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 8: STM PM Parameters

STM PM Parameters	Definition
RS-ES	Displays the number of error seconds in the regenerator section.
RS-ESR	Displays the number of error seconds ratio in the regenerator section.
RS-SES	Displays the number of severely error seconds in the regenerator section.
RS-SESR	Displays the number of severely error seconds ratio in the regenerator section.
RS-BBE	Displays the number of background block errors in the regenerator section.
RS-BBER	Displays the number of background block errors ratio in the regenerator section.

STM PM Parameters	Definition
RS-UAS	Displays the number of unavailable seconds in the regenerator section.
RS-EB	Displays the number of error block in the regenerator section.
MS-ES-L	Displays the number of line error seconds on the node.
MS-ESR-L	Displays the number of line error seconds ratio on the node.
MS-SES-L	Displays the number of line severely error seconds on the node.
MS-SESR-L	Displays the number of line severely error seconds ratio on the node.
MS-BBE-L	Displays the number of line background block errors on the node.
MS-BBER-L	Displays the number of line background block errors ratio on the node.
MS-UAS-L	Displays the number of line unavailable seconds on the node.
MS-EB-L	Displays the number of line error block on the node.

Step 4 Return to your originating procedure.

View Virtual Concatenation (VC) PM Parameters Using CTC

Purpose	This procedure displays the Virtual Concatenation (VC) PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **SDH** > **VC Current Values** tab to view the current PM parameter names.

Step 3 Click the **VC Historical** tab to view the PM parameter names that appear in the Parameter column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 9: VC PM Parameters

VC PM Parameters	Definition
MS-ES	Displays the number of error seconds on the node.

VC PM Parameters	Definition
MS-ESR	Displays the number of error seconds ratio on the node.
MS-SES	Displays the number of severely error seconds on the node.
MS-SESR	Displays the number of severely error seconds ratio on the node.
MS-BBE	Displays the number of background block errors on the node.
MS-BBER	Displays the number of background block errors ratio on the node.
MS-UAS	Displays the number of unavailable seconds on the node.
MS-EB	Displays the number of error block on the node.

Step 4 Return to your originating procedure.

View Ethernet PM Parameters Using CTC

Purpose	This procedure displays the Ethernet PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **Ethernet** > **Current Value** tab to view the current PM parameter names.

Step 3 Click the **Historical** tab to view the PM parameter names that appear in the Parameter column.

Note

The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Ethernet PM Parameters	Definition
rxTotalPkts	Display the total number of packets received.
etherStatsOctets	Displays the total number of octets of data received in the network.
etherStatsOversizePkts	Displays the total number of packets received that were longer than 9618 octets and were otherwise well formed.
dot3StatsFcsErrors	Displays the number of frames with frame check errors.
dot3StatsFrameTooLong	Displays the number of packets that are at least 64 octets long, without a bad FCS, where the 802.3 length/type field did not match the computed DATA field length.
etherStatsJabbers	Displays the total number of packets received that were longer than 9618 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsPkts 64 Octets	Displays the total number of packets received that were 64 octets in length.
etherStatsPkts65to127 Octets	Displays the total number of packets received that were between 65 and 127 octets in length.
etherStatsPkts128to255 Octets	Displays the total number of packets received that were between 128 and 255 octets in length.
etherStatsPkts256to511 Octets	Displays the total number of packets received that were between 256 and 511 octets in length.
etherStatsPkts512to1023 Octets	Displays the total number of packets received that were between 512 and 1023 octets in length.
etherStatsPkts1024to1518 Octets	Displays the total number of packets received that were between 1024 and 1518 octets in length.
ifInUcastPkts	Displays the number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInMcastPkts	Displays the total number of multicast frames received error-free.
ifInBcastPkts	Displays the number of packets delivered to a higher sub-layer and addressed to a broadcast address at this sub-layer.
ifOutUcastPkts	Displays the total number of packets that

Ethernet PM Parameters	Definition
	higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutMcastPkts	Displays the number of multicast frames transmitted error-free.
ifOutBcastPkts	Displays the number of packets requested by higher-level protocols and addressed to a broadcast address at this sub-layer, including that are not transmitted.
TxTotalPkts	Displays the number of transmitted packets.
IfOutOctets	Displays the total number of octets transmitted out of the interface, including framing characters.
etherStatsPkts	Displays the total number of ethernet packets received.
ifInOctets	Displays the total number of octets of received data.
ifInErrors	Displays the total number of packet errors.
etherStatsMulticastPkts	Displays the total number of ethernet multicast packets.
etherStatsBroadcastPkts	Displays the total number of ethernet broadcast packets.
etherStatsUndersizePkts	Dispalys the total number of undersize ethernet packets.

Step 4 Return to your originating procedure .

View OTU PM Parameters Using CTC

Purpose	This procedure displays the OTU PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View** , double-click the line card.

Step 2 Click the **Performance** > **OTU** > **OTU Current Values** tab to view the current PM parameter names.

Step 3 Click the **OTU Historical** tab to view the PM parameter names that appear in the Parameter column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 10: OTU PM Parameters

OTU PM Parameters	Definition
BBE-S	Displays the number of section monitor background block errors on the node.
BBER-S	Displays the number of section monitor background block error ratio on the node.
ES-S	Displays the number of section monitor error seconds on the node.
ESR-S	Displays the number of section monitor error seconds ratio on the node.
FC-S	Displays the number of section monitor failure count on the node.
SES-S	Displays the number of section monitor severely error seconds on the node.
SESR-S	Displays the number of section monitor severely error seconds ratio on the far end node.
UAS-S	Displays the number of section monitor unavailable seconds on the far end node.

Step 4 Return to your originating procedure.

View FEC PM Parameters Using CTC

Purpose	This procedure displays the FEC PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **OTU** > **FEC Current Values** tab to view the current PM parameter names.

Step 3 Click the **FEC Historical** tab to view the PM parameter names that appear in the Parameter column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 11: FEC PM Parameters

FEC PM Parameters	Definition
EC-BITS	Displays the number of bit errors that are corrected by the system.
UC-WORDS	Displays the number of words that are not corrected by the system.

Step 4 Return to your originating procedure.

View ODU PM Parameters Using CTC

Purpose	This procedure displays the ODU PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **ODU** > **Current Values** tab to view the current PM parameter names.

Step 3 Select the **Layer Name** from the drop down menu. The available options are path and gfp. The displayed ODU PM parameters differ based on the option selected here.

The gfp option is currently not supported.

Step 4 Click the **Historical** tab to view the PM parameter names that appear in the Parameter column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 12: ODU PM Parameters when the Layer Name option is path

ODU PM Parameters	Definition
BBE-P	Displays the number of path monitor background block errors on the node.
BBER-P	Displays the number of path monitor background block errors ratio on the node.
ES-P	Displays the number of path monitor error seconds on the node.

ODU PM Parameters	Definition
ESR-P	Displays the number of path monitor error seconds ratio on the node.
FC-P	Displays the number of path monitor failure count on the node.
SES-P	Displays the number of path monitor severely error seconds on the node.
SESR-P	Displays the number of path monitor severely error seconds ratio on the node.
UAS-P	Displays the number of path monitor unavailable seconds on the node.

Table 13: ODU PM Parameters when the Layer Name option is gfp

ODU PM Parameters	Definition
gfpStatsRxSBitErrors	Displays the number of received GFP frames with single bit errors in the core header.
gfpStatsRxTypeInvalid	Displays the number of received GFP frames with invalid type in the core header.
gfpStatsRxCRCErrors	Displays the number of superblock CRC errors with the receive transparent GFP frame.
gfpStatsRxLFDRaised	Displays the number of LFD (Loss of Frame Delineation) raised.
gfpStatsRxCSFRaised	Displays the number of receive client management frames with client signal fail indication.

Step 5 Return to your originating procedure.

View TCM PM Parameters Using CTC

Purpose	This procedure displays the TCM PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** > **TCM** > **Current Values** tab to view the current PM parameter names.

Step 3 Select the **Controller Name** from the drop down menu. The TCM parameters for the selected controller are displayed.

Step 4 Click the **Historical** tab to view the PM parameter names that appear in the Parameter column.

Note The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.

Table 14: TCM PM Parameters

TCM PM Parameters	Definition
BBE-P	Displays the number of path monitor background block errors on the node.
BBER-P	Displays the number of path monitor background block errors ratio on the node.
ES-P	Displays the number of path monitor error seconds on the node.
ESR-P	Displays the number of path monitor error seconds ratio on the node.
FC-P	Displays the number of path monitor failure count on the node.
SES-P	Displays the number of path monitor severely error seconds on the node.
SESR-P	Displays the number of path monitor severely error seconds ratio on the node.
UAS-P	Displays the number of path monitor unavailable seconds on the node.

Step 5 Return to your originating procedure.

View PM Counts at 15-Minute/1Day Intervals Using CTC

Purpose	This procedure provides instructions to change the PM counts for 15-minute/1day intervals using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** tab.

Step 3 Click the relevant sub-tabs to change the PM interval to 15-minute/1day for a controller,

Step 4 (For the NCS4K-2H-OK card) From the **Lane No**. drop-down list, choose an option. The PM value in the table gets updated accordingly.

Step 5 (For the ODU controller) From the **Layer Name** drop-down list, choose an option.

Note Permon (Performance Monitoring) should be enabled for ODU controllers.

Step 6 From the **Controller Name** drop-down list, choose a **controller**.

Step 7 From the **TCM** drop-down list, choose an option. This drop-down list is applicable only for TCM pane.

Note Permon (Performance Monitoring) should be enabled for TCM controllers.

Step 8 Click the **15 min/1Day** radio button.

Step 9 Click **Refresh**.

Step 10 View the **Current** column to find PM counts for the current 15-minute/1day interval.

Note Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute/1day interval, a threshold-crossing alerts (TCA) is raised. The number represents the counter value for each specific PM parameter.

Step 11 View the **Prev-n** columns to find PM counts for the previous 15-minute/1day intervals.

Step 12 Return to your originating procedure.

View Near-End/Far-End PM Counts Using CTC

Purpose	This procedure provide instructions to display the near-end/far-end PM counts for the selected card and port using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** tab.

Step 3 Click the relevant sub-tabs to view the near-end/far-end PM counts for a controller.

Step 4 (For the NCS4K-2H-OK card) From the **Channel No**. drop-down list, choose an option. The PM value in the table gets updated accordingly.

Step 5 (For the ODU controller) From the **Layer Name** drop-down list, choose an option.

Note Permon (Performance Monitoring) should be enabled for ODU controllers.

Step 6 From the **Controller Name** drop-down list, choose a **controller**.

Step 7 From the **TCM** drop-down list, choose an option. This drop-down list is applicable only for TCM pane.

Note Permon (Performance Monitoring) should be enabled for TCM controllers.

Step 8 Click the **Near End/ Far End** radio button (when available).

Note Viewing near-end/far-end PM counts is not available on some tabs.

Step 9 Click **Refresh**.

Note View the Curr (Current) column to find PM counts for the current time interval and Prev-n columns to find PM counts for the previous time intervals respectively

Step 10 Return to your originating procedure.

Reset Current PM Counts Using CTC

Purpose	This procedure provide instructions to reset the current PM counts using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** tab.

Step 3 Click the relevant subtabs to reset the PM counts for a controller.

Step 4 (For the NCS4K-2H-OK card) From the Channel No. drop-down list, choose an option. The PM value in the table gets updated accordingly.

Step 5 (For the ODU controller) From the Layer Name drop-down list, choose an option.

Note Permon (Performance Monitoring) should be enabled for ODU controllers.

Step 6 From the Controller Name drop-down list, choose a controller.

Step 7 Select a PM count column from the table.

Step 8 Click **Baseline**.

Note The Baseline button clears the PM counts that appear in the current time interval at the node level but does not clear the PM counts at the controller level. To check the rate at which PM values are changing, click Refresh after setting the baseline. The baseline values are discarded if you switch to a different tab and then return to the current tab.

Step 9 In the Baseline Statistics dialog box, click one of the following radio buttons:

- **All statistics for port or controller x** - Clears the selected PM counts for the selected port or controller. This means that all time intervals, directions, and signal type counts are reset from the card and the window. View the Curr (Current) column to find PM counts for the current time interval and Prev-n columns to find PM counts for the previous time intervals.
- **All statistics for card** - Clears all the PM counts for all the controllers on the given card.

Step 10 Return to your originating procedure.

Clear Selected PM Counts Using CTC

Purpose	Clear selected PM counts allow to clear the specific PM counts for a specific port at node level. This procedure provide instructions to clear the selected PM counts using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** tab.

Step 3 Click the relevant subtabs and click **Clear** to clear the selected PM counts for a controller.

Step 4 (For the NCS4K-2H-OK) From the Channel No. drop-down list, choose an option. The PM value in the table gets updated accordingly.

Step 5 (For the ODU controller) From the Layer Name drop-down list, choose an option.

Note Permon (Performance Monitoring) should be enabled for ODU controllers.

Step 6 From the Controller Name drop-down list, choose a **controller**.

Step 7 Select a port and click **Clear** to clear the specific PM counts for a specific port at node level. Verify that the selected PM counts have been cleared.

Step 8 Return to your originating procedure.

Set the Auto-Refresh Interval for Displayed PM Counts Using CTC

Purpose	This procedure provide instructions to set the auto-refresh interval for displayed PM counts using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Performance** tab.

Step 3 Click the relevant sub-tabs to set the PM auto-refresh interval for a controller.

Step 4 (For the NCS4K-2H-OK From the **Channel No**. drop-down list, choose an option. The PM value in the table gets updated accordingly.

Step 5 (For the ODU controller) From the **Layer Name** drop-down list, choose an option. This drop-down list is applicable only for ODU controller.

Note Permon (Performance Monitoring) should be enabled for ODU controllers.

Step 6 From the **Controller Name** drop-down list, choose a controller.

Step 7 From the **TCM** drop-down list, choose an option. This drop-down list is applicable only for TCM pane.

Note Permon (Performance Monitoring) should be enabled for TCM controllers.

Step 8 From the **Auto-Refresh** drop-down list, choose an option to refresh the table in the selected interval automatically. The available options are :

- None.
- 15 Seconds.
- 30 Seconds.
- 1 Minute.
- 3 Minutes.
- 5 Minutes.

The PM counts for the newly selected auto-refresh time interval appears.

Note Based on the selected auto-refresh interval, the displayed PM counts automatically get refreshed when each refresh interval completes. If the auto-refresh interval is set to None, the PM counts that appear are not updated unless you click Refresh.

Step 9 Return to your originating procedure.

Set the PM Threshold Values Using CTC

Purpose	This procedure provides instructions to sets the PM threshold values using CTC.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Provisioning > PM Thresholds** tab.

Step 3 Click the relevant sub-tabs.

The sub-tabs are:

- Optics
- SD FEC
- OC
- STS
- STM
- VC
- Ethernet
- HD FEC
- ODU
- OTU
- TCM
- TCA

Step 4 Select a cell, to modify the selected PM threshold for a controller.

Note Verify that the PM thresholds value has been modified.

Step 5 Double-click the selected cell and modify it.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure.

Reset PM Thresholds Using CTC

Purpose	This procedure provide instructions to reset the PM thresholds using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Provisioning** > **PM Thresholds** tab.

Step 3 Click **Reset to Default**.

Note All the threshold values of the selected controller are set to their default values. Verify that the PM thresholds have been reset.

Step 4 Return to your originating procedure.

Refresh PM Threshold at 15-Minute/ 1Day Intervals Using CTC

Purpose	This procedure provide instructions to change the PM Threshold in 15-minute/ 1day intervals using CTC.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Provisioning** tab.

Step 3 Click the relevant sub-tabs to change the PM Threshold interval to 15-minute/ 1day for a controller.

Step 4 (For the ODU controller) From the **Layer Name** drop-down list, choose an option.

Step 5 (For the ODU controller) From the **Controller Name** drop-down list, choose an option.

Step 6 Click the **15 Min/ 1Day** radio button.

Step 7 Click **Refresh**.

Note PM thresholds appear at 15-minute/ 1day intervals in the populated table.

Step 8 Return to your originating procedure.

CHAPTER 9

Smart Licensing

This chapter describes the procedures to configure and verify smart licensing.

Smart Licensing Overview

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

Smart Licensing helps simplify three core functions:

- **Purchasing**: The software that you have installed in your network can be registered, without Product Activation Keys (PAKs).
- **Management**: You can automatically track activations against your license entitlements. Additionally, there is no need to install the license file on every node. You can create license pools (logical grouping of licenses) to reflect your organization structure. Smart Licensing offers you Cisco Smart Software Manager, a centralized portal that enables you to manage all your Cisco software licenses from one centralized website. Cisco Smart Software Manager Overview provides details.
- **Reporting**: Through the portal, Smart Licensing offers an integrated view of the licenses you have purchased and what has been actually deployed in your network. You can use this data to make better purchase decisions, based on your consumption.

Smart Licensing Features

- Your device initiates a call home and requests the licenses it needs.
- Pooled licences - licences are company account-specific, and can be used with any compatible device in your company. You can activate or deactivate different types of licenses on the device without actually installing a license file on the device.
- Licenses are stored securely on Cisco servers accessible 24x7x365.
- Licenses can be moved between product instances without a license transfer. This greatly simplifies the reassignment of a software license as part of the Return Material Authorization (RMA) process.

- Complete view of all Smart Software Licenses used in the network using a consolidated usage report of software licenses and devices in one easy-to-use portal.

Cisco Smart Account

Cisco Smart Account is an account where all products enabled for Smart Licensing are deposited. Cisco Smart Account allows you to manage and activate your licenses to devices, monitor license use, and track Cisco license purchases. Through transparent access, you have a real-time view into your Smart Licensing products. IT administrators can manage licenses and account users within your organization's Smart Account through the Smart Software Manager.

When creating a Smart Account, you must have the authority to represent the requesting organization. After submitting, the request goes through a brief approval process. See http://software.cisco.com to learn about, set up, or manage Smart Accounts.

Cisco Smart Software Manager Overview

Cisco Smart Software Manager enables you to manage all of your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances). Use the Cisco Smart Software Manager to do the following tasks:

- Create, manage or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

Virtual Accounts

A Virtual Account exists as a sub-account withing the Smart Account. Virtual Accounts are a customer-defined structure based on organizational layout, business function, geography or any defined hierarchy. They are created and maintained by the Smart Account administrator. Smart Licencing allows you to create multiple license pools or virtual accounts within the Smart Software Manager portal. Using the Virtual Accounts option you can aggregate licenses into discrete bundles associated with a cost center so that one section of an organization cannot use the licenses of another section of the organization. For example, if you segregate your company into different geographic regions, you can create a virtual account for each region to hold the licenses and product instances for that region.

All new licenses and product instances are placed in the default virtual account in the Smart Software Manager, unless you specify a different one during the order process. Once in the default account, you may choose to transfer them to any other account as desired, provided you have the required access permissions.

Use the Smart Software Manager portal to create license pools or transfer licenses.

Product Instance Registration Tokens

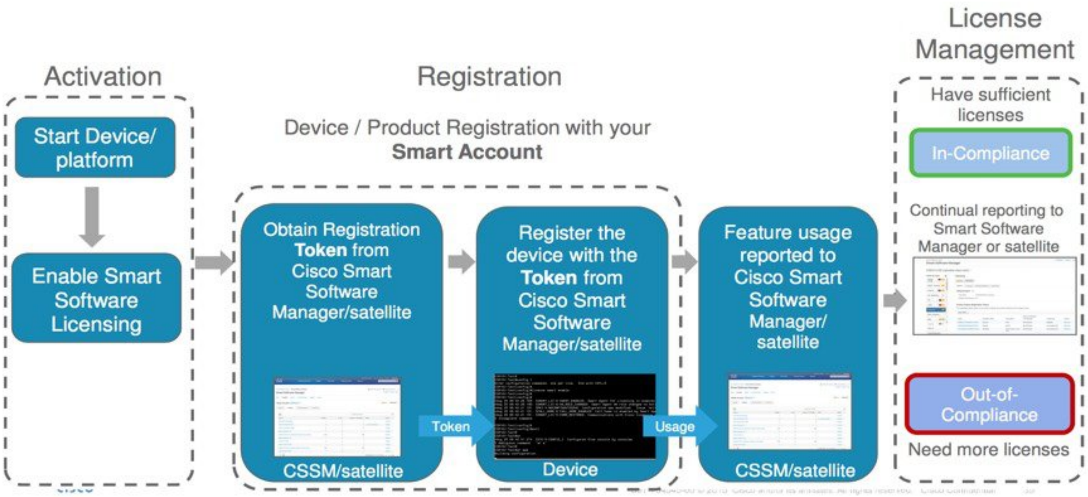
A product requires a registration token until you have registered the product. On successful registration , the device receives an identity certificate . This certificate is saved and automatically used for all future communications with Cisco. Registration tokens are stored in the Product Instance Registration Token Table associated with your enterprise account. Registration tokens can be valid from 1 to 365 days.

Product Instances

A product instance is an individual device with a unique device identifier (UDI) that is registered using a product instance registration token (or registration token). You can register any number of instances of a product with a single registration token. Each product instance can have one or more licenses residing in the same virtual account. Product instances must periodically connect to the Cisco Smart Software Manager servers during a specific renewal period. If you remove the product instance, its licenses are released and made available within the virtual account.

The figure below depicts a working model of Smart Licensing that involves a three-step procedure.

Figure 1: Smart Licensing Work Flow


Activation
Start Device/ platform
Enable Smart Software Licensing
Registration
Device / Product Registration with your Smart Account
Obtain Registration Token from Cisco Smart Software Manager/satellite
CSSM/satellite
Token
Register the device with the Token from Cisco Smart Software Manager/satellite
Device
Usage
Feature usage reported to Cisco Smart Software Manager/ satellite
CSSM/satellite
License Management
Have sufficient licenses
In-Compliance
Continual reporting to Smart Software Manager or satellite
Out-of-Compliance
Need more licenses

1. **Setting up Smart Licensing**: You can place the order for Smart Licensing, to manage licenses on Cisco.com portal. You agree to the terms and conditions governing the use and access of Smart Licensing in the Smart Software Manager portal.

2. **Enabling and Use Smart Licensing**: Smart Licensing is enabled by default. You can use either of the following options to communicate:

   - **Smart Call Home**: The Smart Call Home feature is automatically configured when Smart Licensing is enabled. Smart Call Home is used by Smart Licensing as a medium for communication with the Cisco license service. Call Home feature allows Cisco products to periodically call-home and perform an audit and reconciliation of your software usage information. This information helps Cisco efficiently track your install base, keep them up and running, and more effectively pursue service and support contract renewals, without much intervention from your end. For more information on Smart Call Home feature, see http://www.cisco.com/c/dam/en/us/td/docs/switches/lan/smart_call_home/SCH_Deployment_Guide.pdf.

   - **Smart Software Manager Satellite** : is a component of Cisco Smart Licensing and works in conjunction with Cisco Smart Software Manager (SSM). It helps customers intelligently manage product licenses, providing near real-time visibility and reporting of the Cisco licenses they purchase and consume.

     For security-sensitive customers who do not want to manage their installed base using a direct Internet connection, the Smart Software Manager satellite is installed on the customer premises and provides a subset of Cisco SSM functionality. After you download the satellite application, deploy it, and register it to Cisco SSM, you can perform the following functions locally:

- Activate or register a license
- Get visibility to your company's licenses
- Transfer licenses between company entities

Periodically, the satellite needs to synchronize with Cisco SSM to reflect the latest license entitlements.

For more information about Smart Software Manager satellite, see http://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.

3. **Manage and Report Licenses**: You can manage and view reports about your overall software usage in the Smart Software Manager portal. Compliance reporting describes the types of Smart Licensing reports.

Consumption Model

The consumption model is a new pricing model for line cards. This provides a flexible deployment model with the ability to increase bandwidth to meet your demands. The consumption model is described in the table below.

<table>
<tr><th>License/PID</th><th>Description</th><th>Consumption</th></tr>
<tr><td>NCS4K-4H-OPW-LO</td><td>Licensed PID for NCS4K-4H-OPW-QC2 card. This license is available when the card is purchased.</td><td>This is a licensed PID for OTN that allows 100G of bandwidth per line card.</td></tr>
<tr><td>S-CFP2-WDM-LIC</td><td>Software license for WDM CFP2 pluggable port. This software license needs to be purchased if the WDM CFP2 ports are configured.</td><td>If the DWDM interface is enabled on the NCS4K-4H-OPW-LO licensed PID, then this license is consumed. A maximum of two licenses can be consumed per licensed PID as shown below:
<table>
<tr><th>Port Bandwidth</th><th>WDM CFP2 Pluggable Port
S-CFP2-WDM-LIC</th></tr>
<tr><td>200G</td><td>1</td></tr>
<tr><td>100G</td><td>1</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>License/PID</th><th>Description</th><th>Consumption</th></tr>
<tr><td>S-NCS4K-100G-LIC</td><td>Software license for 100G bandwidth usage. This software license needs to be purchased for subsequent 100G bandwidth usage. The basis for the calculation is the running configuration of the router.</td><td>For every additional 100 G chunk of bandwidth usage this license is consumed per NCS4K-4H-OPW-LO licensed PID. A few examples of the consumption scale is shown below:
<table>
<tr><th>Port Bandwidth</th><th>100G Bandwidth Licenses Consumed
S-NCS4K-100G-LIC</th></tr>
<tr><td>1 x 200G</td><td>2</td></tr>
<tr><td>1 x 100G</td><td>1</td></tr>
<tr><td>1 to 2 x 40G</td><td>1</td></tr>
<tr><td>3 to 5 x 40G</td><td>2</td></tr>
<tr><td>1 to 10 x 10G</td><td>1</td></tr>
<tr><td>11 to 20 x 10G</td><td>2</td></tr>
</table></td></tr>
<tr><td>S-NCS4K-POTS</td><td>License POTS - one per line card. This software license needs to be purchased when carrier ethernet or MPLS packet features are activated.</td><td>This license is consumed when carrier ethernet or MPLS packet features are enabled for the licensed PID.</td></tr>
</table>

Configure Smart Software Licensing Using CTC

Purpose	This procedure enables you to register or deregister the router in the Cisco Smart Software Manager. You can also manually renew the authorization and ID certificate for your device.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click **Provisioning** > **Smart Licensing** > **Smart Software Licensing** tabs.

Step 2 To register the device, perform Steps 6 through 9.

Step 3 To deregister the device, perform Steps 10 and 11.

Step 4 To renew ID certificate, perform Step 12.

Step 5 To renew authorization, perform Step 13.

Step 6 Login to your smart account in Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory) or smart software manager satellite using the Cisco provided username and password.

Step 7 Generate a product instance registration token. Copy or download the token to a text file.

The token is used to register and activate a device, and assign the device to a virtual account.

Step 8 Click **Register**.

The Smart Software Licensing Product Registration dialog appears.

Step 9 Paste the token you copied in Step 7 and click **OK**.
A message is displayed that the product registration has initiated successfully. The smart licensing software status is updated. The details in the Provisioning > Smart Licensing > Smart Licensing Usage tab is also updated if the card is in use.

In case an invalid token is used, the registration process fails and the status is displayed in the smart licensing software status area. You can attempt to register the device again by using the correct token.

In the event of a communication failure between the device and the portal or satellite, CTC waits for 24 hours before attempting to register the device again. You can use the " Force Register " button to try registering the device again instead of waiting for 24 hours.

Step 10 To cancel the registration of your device, click **Deregister**.

A Confirm Deregistration dialog is displayed.

Step 11 Click **OK**.

A message is displayed after the device is successfully deregistered.

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 the Deregister option to cancel the registration on your device. All Smart Licensing entitlements and certificates on the platform are removed.

Note Though the product instance has been de-registered from the Cisco license cloud service, Smart Licensing is still enabled.

Step 12 To manually renew your ID certificate, click **Renew ID Cert**.

A message is displayed after the renewal of the ID certificate is complete.

Note 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.

Step 13 To manually renew the authorization, click **Renew Authorization**.

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 the Renew Authorization option to make an on-demand manual update of your registration. Thus, instead of waiting 30 days for the next registration renewal cycle, you can issue this command 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 the Renew Authorization option to retry the authorization period renewal. If the retry is successful, a new authorization period begins.

Stop. You have completed this procedure.

Configure Call Home

Purpose	Call Home provides an email and HTTP/HTTPS based notification for critical system policies. A predefined destination is provided for sending alerts to the Cisco TAC. This procedure enables you configure the HTTP proxy server and also add or remove destination HTTP/HTTPS addresses of the Cisco Smart Software Manager or satellite.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click **Provisioning** > **Call Home** tabs.

Step 2 To configure the HTTP proxy server, perform Steps 4 and 5.

Step 3 To add or delete a destination HTTP/HTTPS address, perform Step 6.

By default the destination HTTPS address of the Cisco Smart Software Manager for the CiscoTAC-1 profile is https://tools.cisco.com/its/service/oddce/services/DDCEService.

Step 4 Check the **Use HTTP Proxy** checkbox.

The Port Number field is enabled.

Step 5 Specify the port of the HTTP proxy server. The range is 1 to 65535.

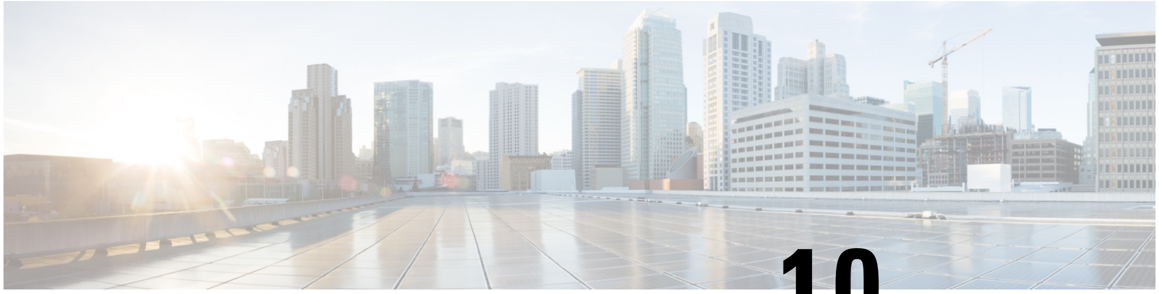
Step 6 Click **Create.**

The Create Destination Address dialog is displayed.

Step 7 Specify the URL and click **OK**.

To remove any of the specified destination addresses, select the address from the list and click **Delete**.

Stop. You have completed this procedure.



CHAPTER 10

Manage Alarm Profiles

This chapter provides the CTC procedures to create, load and store the alarm profiles. This chapter also provides procedures to change the default alarm severities and apply an alarm profile to a card or to the node.

Alarm Severities

Alarm severities follow the Telcordia GR-474-CORE standard, so a condition might be Alarmed at a severity of Critical [CR], Major [MJ], or Minor [MN]), Not Alarmed (NA), or Not Reported (NR). These severities are reported in the CTC software Alarms, Conditions, and History windows at all levels: network, shelf, and card.

The users can create their own profiles with different settings for some or all conditions and apply these wherever desired. (See the Alarm Profiles, on page 139 section.) For example, in a custom alarm profile, the default severity of a signal loss on data interface (SIGLOSS) alarm on an Ethernet port could be changed from major to critical.

Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ports, cards, or nodes. A created alarm profile can be applied to any node on the network. Alarm profiles can be saved to a file and imported elsewhere in the network, but the profile must be stored locally on a node before it can be applied to the node or its cards.

CTC can store up to ten active alarm profiles at any time to apply to the node.

Alarm Severity Options

To change or assign alarm severity, left-click the alarm severity you want to change in the alarm profile column. Seven severity levels appear for the alarm:

- Not Reported (NR)
- Not Alarmed (NA)
- Minor (MN)
- Major (MJ)
- Critical (CR)
- Use Default

Use Default severity levels only appear in alarm profiles. They do not appear when you view alarms, history, or conditions.

Apply Alarm Profiles

In the CTC node view, the **Alarm Behavior** window displays alarm profiles for the entire node and specific cards. In the card view, the Alarm Behavior window displays the alarm profiles for the selected card. Alarm profiles form a hierarchy. A node-level alarm profile applies to all cards in the node except cards that have their own profiles. A card-level alarm profile applies to all ports on the card.

At the node level, you can apply profile changes on a card-by-card basis or set a profile for the entire node.

Create a New Alarm Profile Using CTC

Purpose	This procedure enables you to create a new alarm profile.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Software Installation Guide for Cisco NCS 4000 Series
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In Node View/Card View , click the **Provisioning** > **Alarm Profiles** > **Alarm Profile Editor** tabs .

Note To access the profile editor from Network View, click **Provisioning** > **Alarm Profile** tabs.

Step 2 Click **New**.

Step 3 In the **New Profile** dialog box enter profile name in the **New Profile Name** field.

Note Profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name.

Step 4 Click **OK**. A new alarm profile is created.

Note Up to ten profiles can be stored in CTC.

Step 5 (Optional) Complete step4 and step5 in Set the Severity of Alarms Using CTC, on page 143 to modify the default severity of alarm(s) in the profile.

Step 6 Select the profile you want to save and click **Store**.

Alternatively you can right-click the profile column and click **Store** from the short cut menu.

Step 7 In the **Store Profile(s)** dialog box, perform the following:

a) Select **To Node(s)** option and choose the node(s) were you want to save the profile.

Alternatively select **To File** option to save profile in a file.

b) Click **OK**.

Step 8 Click **Available**. The new profile will now be present in the list of available profiles.

Stop. You have completed this procedure.

Clone an Alarm Profile Using CTC

Purpose	This procedure enables you to create clone of an existing alarm profile.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Software Installation Guide for Cisco NCS 4000 Series
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In Node/Card View, click the **Provisioning** > **Alarm Profiles** > **Alarm Profile Editor** tabs .

Note To access the profile editor from Network View, click **Provisioning** > **Alarm Profile** tabs.

Step 2 Complete Load an Alarm Profile Using CTC, on page 142, to load an alarm profile.

Step 3 Right-click anywhere in the loaded profile entry. The short cut menu appears.

Step 4 Click **Clone** option.

Step 5 (Optional) Complete steps 3 and 4 in Set the Severity of Alarms Using CTC, on page 143 to modify the default severity of alarm(s) in the profile.

Step 6 In the **Store Profile(s)** dialog box, perform the following:

a) Select **To Node(s)** option and choose the node(s) were you want to save the profile.

   Alternatively select **To File** option to save profile in a file.

b) Click **OK**.

Step 7 Click **Available**. The cloned profile will now be present in the list of available profiles.

Stop. You have completed this procedure.

Load an Alarm Profile Using CTC

Purpose	This procedure enables you to downloads an alarm profile from a node or a file.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Software Installation Guide for Cisco NCS 4000 Series
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In Node/Card View , click the **Provisioning** > **Alarm Profiles** > **Alarm Profile Editor** tabs .

Note To access the profile editor from Network View, click **Provisioning** > **Alarm Profile** tabs.

Step 2 Click **Load**. The Load Profile(s) dialog box appears.

Step 3 If you want to download a profile from a node, click **From Node** option and perform the following:

a) Select a node from the **Node Names** list.
   The **Profile Names** list on the right, is updated with the alarm profiles saved on the selected node.

b) Select the name of the profile from the **Profile Names** list.

Step 4 If you want to download a profile from a file, click **From File** option.

Step 5 Click **OK.**

The downloaded profile appears in the Alarm Profiles window.

Stop. You have completed this procedure.

Set the Severity of Alarms Using CTC

Purpose	This procedure enables you to set the severity of alarms using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In Node/Card View , click the **Provisioning** > **Alarm Profiles** > **Alarm Profile Editor** tabs .

Note To access the profile editor from Network View, click **Provisioning** > **Alarm Profile** tabs.

Step 2 Complete Load an Alarm Profile Using CTC, on page 142, to load an alarm profile.

Step 3 Select an alarm in the profile and choose severity from the drop-down list.

Refer to the following guidelines when you view the alarms or conditions after making modifications:

- All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474-CORE.
- Default severities are used for all alarms and conditions until you create and apply a new profile.
- Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Note Repeat step3 to update multiple alarms.

Step 4 To save the updated profile, select the profile and click **Store**.

Alternatively you can right-click the profile column and click **Store** from the short cut menu.

Step 5 In the **Store Profile(s)** dialog box, perform the following:

a) Select **To Node(s)** option and choose the node(s) were you want to save the profile.

Alternatively select **To File** option and click **Browse** to navigate to the location where you want to save the profile.

b) Click **OK**.

Stop. You have completed this procedure.

Delete Alarm Profile Using CTC

Purpose	This procedure enables you to delete an existing alarm profile saved on a node.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In Node/Card View, click the **Provisioning** > **Alarm Profiles** > **Alarm Profile Editor** tabs .

Note To access the profile editor from Network View, click **Provisioning** > **Alarm Profile** tabs.

Step 2 Click **Delete.**

Note You cannot delete the Active alarm profiles.

Step 3 Click the node name in the **Node Names** list to highlight the profile location.

Tip If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

Step 4 Click the profile names that you want to delete in the **Profile Names** list.

Step 5 Click **OK**.

Stop. You have completed this procedure.

Apply/Suppress an Alarm Profile on a Node Using CTC

Purpose	This procedure enables you to apply/suppress an alarm profile on a node using CTC.

Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** tab.

Step 2 Click **Alarm Profiles** > **Alarm Behavior** tabs.

Step 3 From the **Node Profile** drop down list, select a profile.

Note Select None to detach a profile from the node.

Step 4 Check the **Supress Alarms** checkbox, if you want to suppress the profile for the node.

Step 5 Click **Apply**, to save the changes.

Stop. You have completed this procedure.

Apply/Suppress an Alarm Profile on a Line Card Using CTC

Purpose	This procedure enables you to apply/suppress an alarm profile on a line card using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** tab.

Step 2 Click **Alarm Profiles** > **Alarm Behavior** tabs.

This tab displays the list of line cards.

Step 3 To apply a profile on a line card , click the **Profile** column, and select a profile from the drop down list.

Note Select None to detach a profile from the line card.

Step 4 Check the **Supress Alarms** checkbox, if you want to suppress the profile for the card.

Step 5 Click **Apply**, to save the changes.

Stop. You have completed this procedure.

Apply/Suppress an Alarm Profile on a Port Using CTC

Purpose	This procedure enables you to apply/suppress an alarm profile on a port for NCS4K-20T-O-S, NCS4K-2H-O-K, NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double click the line card.

Step 2 Click **Provisioning** > **Alarm Profiles** > **Alarm Behavior** tabs.

The pane displays the list of port numbers.

Step 3 To apply a profile on a port, click the **Profile** column, and select a profile from the drop down list.

Note Select None to detach a profile from the port.

Step 4 Check the **Supress Alarms** checkbox, if you want to suppress the profile for the port.

Step 5 Click **Apply**, to save the changes.

Stop. You have completed this procedure.

CHAPTER 11

Configure High Availability

This chapter describes the procedures for fast recovery of the system from various faults that can occur in any part of the OTN network.

Hard Reset a card Using CTC

Purpose	Hard reset will allow you to perform reset on a card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the **line card** (NCS4K-20T-O-S/ NCS4K-2H10T-OP-KS/ NCS4K-2H-O-K/ NCS4K-24LR-O-S).

Step 2 Click the **Inventory** tab.

Step 3 Select a card to perform a hard reset.

Step 4 Click **Hard Reset**.

Stop. You have completed this procedure.

LC and RP VM Switchover Using CTC

Purpose	This procedure enables you to perform switchover from active LC/RP VM to standby LC/RP VM.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

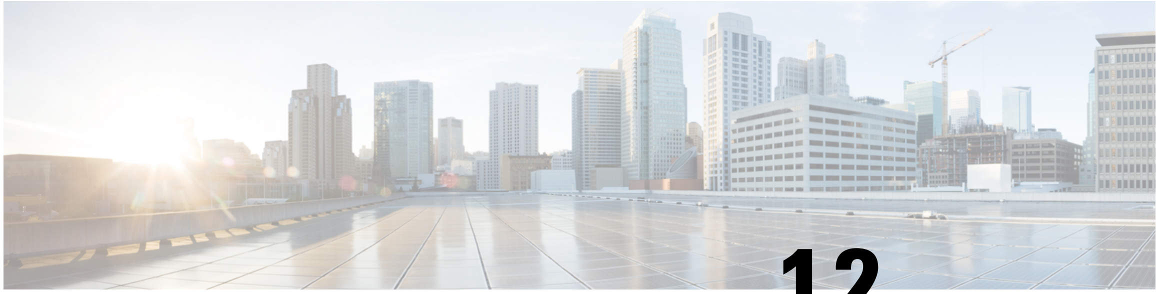
Procedure

Step 1 In the Node View, click the **Maintenance** > **Switchover** tabs.

Step 2 Click **Switchover RP** or **Switchover LC**.

Note If Frequency Synchronization is configured on the node, it will take up to 60 seconds to attain the frequency synchronization lock after VM switchover.

Stop. You have completed this procedure.



CHAPTER 12

Configuring PRBS

This chapter describes the procedure to configure the PRBS.

Understanding PRBS

Pseudo Random Binary Sequence (PRBS) feature allows users to perform data integrity checks on their encapsulated packet data payloads using a pseudo-random bit stream pattern. PRBS generates a bit pattern and sends it to the peer router that uses this feature to detect if the sent bit pattern is intact or not.

Configure PRBS Using CTC

Purpose	This task enables PRBS settings on the source and destination controllers of the circuit. PRBS can also be configured on the card.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Perform Step 2 to provision PRBS on the NCS4K-4H-OPW-QC2 card. Else, proceed with Step 3.

Step 2 In the node view, double-click the card where you want to provision PRBS. The card view appears.

Continue with Step 6.

Step 3 In the network view, click the **OTN** > **Circuits** tabs.

Step 4 To discover the circuits, complete Discover a Circuit Using CTC, on page 86.

Step 5 Select a circuit in ACTIVE state and click **Edit**.

The Edit Circuit dialog displays.

Step 6 Click the **Maintenance** > **PRBS Configuration** tabs.

Step 7 Set the admin state to OOS,MT for the source and destination controllers.

Step 8 From the Mode drop-down list, choose a mode.

Step 9 From the Pattern drop-down list, choose a pattern.

PN23 is not supported on the NCS4K-4H-OPW-QC2 card.

Step 10 Click **Apply**.

Stop. You have completed this procedure.

CHAPTER 13

Configuring Breakout

This chapter gives procedure to configure breakout.

- Understanding Breakout, on page 151
- Configure Breakout Controller Using CTC, on page 151

Understanding Breakout

Breakout is the concept of splitting the higher density port like 100G or 40G to multiple independent and logical ports i.e. 100G->10x10G or 100G->2x40G or 40G->4x10G.This is possible due to multilane architecture of the optics and cables. The standard R/S/I/P format is 4-tuple. 5-tuple interfaces are represented as - R/S/I/P/SP, where SP indicates the breakout port.

The Cisco NCS 4000 series supports the breakout feature. This feature is supported on the following cards:

- NCS4K-4H-OPW-QC2 card-Breakout enables a 40 Gigabit lane of the card to be split into four independent and logical 10 Gigabit Ethernet or OTU2/OTU2e ports. All the QSFP+ ports are break-out capable.
- NCS4K-2H10T-OP-KS card-Using breakout, each 100 Gig lane of NCS4K-2H10T-OP-K can be used by further breaking to 10 G ports. There is no breakout pluggable. 100 G SFP is used for the breakout. Using breakout, each lane of NCS4K-2H10T-OP-KS card can be used separately and as a physical 10G port.

Configure Breakout Controller Using CTC

Purpose	This task provisions the breakout controller for NCS4K-2H10T-OP-KS and NCS4K-4H-OPW-QC2, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Software Installation Guide for Cisco NCS 4000 Series
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 In node view, double-click the line card.

Step 2 Click the **Provisioning** > **Port Modules** tabs.

Step 3 Click **Lane Controllers**.

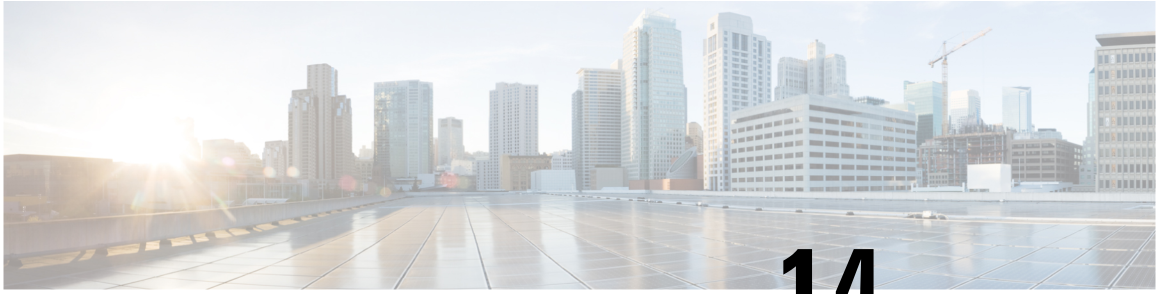
Step 4 In the Lane Controllers dialog box, perform the following steps to configure the breakout controller:

a) Select the port from the drop-down list.

b) Set the PortMode, framing type, and mapping type for the port selected.

c) Click **Apply**.

Stop. You have completed this procedure.



CHAPTER 14

Manage the Node

This chapter provides the CTC procedures for maintaining the nodes, including backup and restoration, viewing the audit trails, and resetting the cards.

Set Up Name, Date, and Time Information Using CTC

Purpose	This procedure provisions identification information
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Insta*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **General** > **General** tabs.

Step 2 Enter the name of the node for which you want to set the date and time in the **Node Name/TID** field.

Step 3 Click **Create**.

CTC makes use of a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node. It ensures that all the network nodes use the same date and time reference. The server synchronizes the nodes time after power outages or software upgrades.

Step 4 In the **Create NTP/SNTP** dialog box, enter the following information:

- Peer/Server—Choose **Peer or Server** from the drop-down list.
- IP Address— Click **IPv4 Address**or **IPv6 Address** radio button. Enter IPv4 or IPv6 address or hostname of the NTP/SNTP server that provides clock synchronization.
- Preferred—Check the check box if the peer is the preferred server that provides clock synchronization.

Step 5 Click **OK** to set the date and time of the node.

Step 6 If you do not want to use the NTP/SNTP server for date and time, complete the date and time fields manually. The node will use these fields for alarm dates and times. By default, CTC displays all the alarms in the CTC computer time zone for consistency. In **Time** area, enter the following information:

- Date—Enter the current date in the MM/DD/YY format, for example, September 24, 2002 is 9/24/2002.
- Time—Enter the current time in the Hours:Minutes:Seconds format, for example, 11:24:58. The node uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.
- Time Zone—Select the required time zone from the drop-down list. Choose a city within your time zone from the drop-down list. The list displays the 80 World Time Zones from -11 through 0 (GMT) to +14. Continental United States time zones are GMT-05:00 (Eastern), GMT-06:00 (Central), GMT-07:00 (Mountain), and GMT-08:00 (Pacific).

Step 7 Click **Apply**.

Stop. You have completed this procedure.

Back Up the Configuration Using CTC

Purpose	This procedure enables you to store a backup version of the Cisco NCS 4000 node configuration on the node's hard disk.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	Required. Cisco recommends performing a configuration backup at approximately weekly intervals and prior to and after configuration changes.
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Procedure

Step 1 In Node View, click the **Maintenance** > **Database** tabs.

Step 2 Click **Backup**. This opens Backup Database dialog box.

Step 3 Enter the backup file name.

Step 4 Click **OK** to save the current configuration on node's hard disk.

Stop. You have completed this procedure.

Restore the Configuration Using CTC

Purpose	This procedure enables you to restore the NCS 4000 configuration from the configuration file on the workstation running CTC or on a network server.
Tools/Equipment	None
Prerequisite Procedures	• "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* • Back Up the Configuration Using CTC, on page 154
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Procedure

Step 1 In Node View, click the **Maintenance** > **Database** tabs.

Step 2 Click **Restore**.

Step 3 Locate the backup configuration file stored on the workstation running CTC or on a network server.

Step 4 Click **Open**.

Step 5 Click **OK** in the confirmation dialog box to restore the NCS 4000 configuration.

Stop. You have completed this procedure.

View and Archive the Audit Trail Records Using CTC

Purpose	This procedure enables you to view and archive audit trail records.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

In NCS 4000, audit trail is used to view the list of all the configuration commands issued to the node. Audit trail records are useful for maintaining security, recovering lost transactions, and enforcing accountability. Accountability refers to tracing user activities; that is, associating a process or action with a specific user.

You need to archive the audit trail logs to maintain a record of actions performed for the node. If the audit trail log is not archived, the oldest entries are overwritten after the log reaches capacity.

Procedure

Step 1 In Node View, click the **Maintenance** > **Audit** tabs.

Step 2 Click **Retrieve**.

The most recent audit trail records appears in the Audit tab.

Step 3 Select a record and Click **Archive**.

The Archive Audit Trail dialog box appears to store the audit trail log entries in a user generated file.

Step 4 Navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File Name field.

Step 6 Click **Save** and click **OK**.

Note Archiving does not delete entries from the CTC audit trail log. However, the entries will be deleted by the system after the log capacity is reached. If you archived the entries, you cannot re-import the log file back into CTC and will have to view the view in a different application such as Microsoft Word.

Stop. You have completed this procedure.

Monitor Environmental Parameters Using CTC

Purpose	This procedure enables you to monitor the en
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Softwar*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **General** tabs.

Step 2 Click the **Power Monitor** sub-tab.

This sub-tab dynamically displays the power consumption values of the NCS 4000 chassis. The values are displayed based on the input voltage going into the system.

- Equipments—Displays the route processors and power filters of the chassis.
- Card number/Equipment Number—Displays the route processor card numbers and power filter numbers.
- Module Sensor—Displays the module sensor name of the selected equipment.
- Value (MilliAmperes)—Displays the module sensor values (in MilliAmperes) of the selected equipment.

Step 3 Click the **Temperature** sub-tab.

This sub-tab displays the input temperature of the NCS 4000 chassis.

- Equipments—Displays the route processors and power filters of the chassis.
- Card number/Equipment Number—Displays the route processor card numbers and power filter numbers.
- Module Sensor—Displays the module sensor name of the selected equipment.
- Value (Celsius)—Displays the module sensor values (in Celsius) of the selected equipment.

Step 4 Click the **Voltage** sub-tab.

This sub-tab displays the input voltage of the NCS 4000 chassis.

- Equipments—Displays the route processors and power sensor name of the module card.
- Card number/Equipment Number—Displays the route processor card numbers and power filter numbers.

Step 5 Click the **Fan Speed** sub-tab.

This sub-tab displays the input values of fan speed supply in the NCS 4000 chassis. The values are displayed based on the input speed going into the fan.

- Equipments—Displays the route processors of the chassis.
- Router name (0/FT0)—Displays all the fan tray names.
- Module Sensor—Displays the speed sensor of the module.
- Value (RPM)—Displays the module sensor speed (in RPM) of the selected equipment.

Stop. You have completed this procedure.

Hard Reset Using CTC

Purpose	This procedure enables you to reset the LC or RP using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser only

Only the hard reset of the card is supported. The hard reset temporarily removes power from the card and clears all the buffer memory.

Procedure

Step 1 In Node View, click the **Inventory** tab.

Step 2 Select the LC or RP.
The **Hard-Reset Card** button gets enabled.

Step 3 Click **Hard-Reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

Stop. You have completed this procedure.

View Equipment Inventory

In Node View, click the Provisioning > Inventory tabs. The tab displays information about the NCS 4000 equipment, including:

- Location—Identifies where the equipment is installed, either chassis or slot number.
- Eqpt Type—Displays the type of equipment.
- Admin State—Changes the service state of the card unless network conditions prevent the change.

  The administrative state changes to OOS,DSBLD when the card is shut down due to insufficient power.
- Description—Displays the description of the equipment.
- Serial #—Displays the equipment serial number; this number is unique to each card.
- Service State—Displays the current card service state, which is an autonomously generated state that gives the overall condition of the card. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.
- Uptime—Displays the time from the last boot.
- Replaceable—Indicates whether an equipment can be replaced or not.
- Product ID—Displays the manufacturing product identifier for a hardware component, such as a fan tray, chassis, or card.
- Version ID—Displays the manufacturing version identifier for a fan tray, chassis, or card.
- HW Part #—Displays the hardware part number; this number is printed on top of the card.
- CLEI—Displays the Common Language Equipment Identifier code.
- PCA#— Displays the Printed Circuit Assembly number.

- HW ID—Displays the hardware identifier of the equipment.

Firewall Ports

The following table lists the ports that must be enabled to establish a communication channel with the NE (controller card).

Table 15: Firewall Ports for Various Sessions

Session Type	Session Description	Mode	Port Number	Fi
HTTP	HTTP port on NE	Standard	80	In
		Secure	443 for SSL	In
SSH	SSH port on NE	Secure	22	In
Telnet	Telnet port on NE	Standard	23	In
TL1	TL1 port on NE	Standard	2361,3082,3083	In
SNMP	SNMP listener port on NE	Standard	161	In
		Secure		
	SNMP trap listener port on the machine receiving the traps	Standard	162 (default); user configurable to any port between 1024 to 65535	C
		Secure		

CHAPTER 15

Configure SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by Cisco NCS 4000 series.

Understand SNMP

SNMP is an application-layer communication protocol that allows Cisco NCS 4000 series network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

NCS 4000 uses SNMP for asynchronous event notification to a network management system (NMS). SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information.

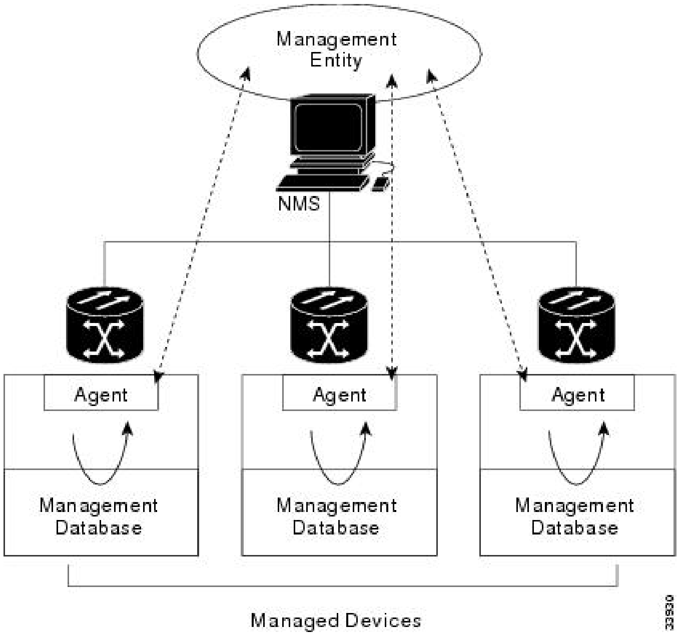
NCS 4000 supports SNMP Version 1 (SNMPv1), SNMP Version 2 (SNMPv2), and SNMP Version 3 (SNMPv3). As compared to SNMPv1, SNMPv2 includes additional protocol operations and 64-bit performance monitoring support. SNMPv3 provides authentication, encryption, and message integrity and is more secure.

Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

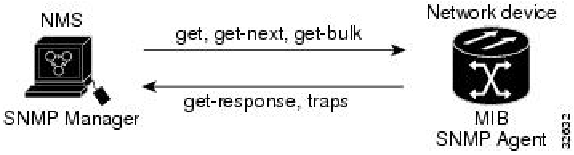
A management system executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or several management systems. The following figure illustrates the relationship between the network manager, the SNMP agent, and the managed devices.

Figure 2: Example of the Primary SNMP Components



An agent (such as SNMP) residing on each managed device translates local management information data—such as performance information or event and error information—caught in software traps, into a readable form for the management system. The following figure illustrates SNMP agent get-requests that transport data to the network management software.

Figure 3: Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.

SNMP Support

- **User-Based Security Model**—The User-Based Security Model (USM) uses the HMAC algorithm for generating keys for authentication and privacy. SNMPv3 authenticates data based on its origin, and ensures that the data is received intact. SNMPv1 and v2 authenticate data based on the plain text community string, which is less secure when compared to the user-based authentication model.

- **View-Based Access Control Model**—The view-based access control model controls the access to the managed objects. RFC 3415 defines the following five elements that VACM comprises:
  - Groups—A set of users on whose behalf the MIB objects can be accessed. Each user belongs to a group. The group defines the access policy, notifications that users can receive, and the security model and security level for the users.
  - Security level—The access rights of a group depend on the security level of the request.
  - Contexts—Define a named subset of the object instances in the MIB. MIB objects are grouped into collections with different access policies based on the MIB contexts.
  - MIB views—Define a set of managed objects as subtrees and families. A view is a collection or family of subtrees. Each subtree is included or excluded from the view.
  - Access policy—Access is determined by the identity of the user, security level, security model, context, and the type of access (read/write). The access policy defines what SNMP objects can be accessed for reading, writing, and creating.

Access to information can be restricted based on these elements. Each view is created with different access control details. An operation is permitted or denied based on the access control details.

You can configure SNMPv3 on a node to allow SNMP get and set access to management information and configure a node to send SNMPv3 traps to trap destinations in a secure way. SNMPv3 can be configured in secure mode, non-secure mode, or disabled mode.

SNMP, when configured in secure mode, only allows SNMPv3 messages that have the authPriv security level. SNMP messages without authentication or privacy enabled are not allowed. When SNMP is configured in non-secure mode, it allows SNMPv1, SNMPv2, and SNMPv3 message types.

SNMP Traps

The uses SNMP traps to generate all alarms and events, such as raises and clears. The traps contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port).
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service-affecting).
- Date and time stamp showing when the alarm occurred.

Create Group Access Using CTC

Purpose	This procedure enables you to create a user group and configure the access parameters for the users in the group.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **Group Access** tabs.

Step 2 Click **Create**.

Step 3 In the Create Group Access dialog box, enter the following information:

- Group Name—The name of the SNMP group, or collection of users, who share a common access policy.
- SNMP Version—Version of SNMP. The possible values are SNMPv1, SNMPv2, and SNMPv3.
- Security Level—The security level for which the access parameters are defined. You can configure the security level only when SNMPv3 is selected. Select from the following options:
  - noAuthNoPriv—Uses a user name match for authentication.
  - authNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - authPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.
- Views
  - Read View Name—Read view name for the group.
  - Notify View Name—Notify view name for the group.
  - Write View Name—Write view name for the group.

Step 4 Click **OK** to save the information.

Stop. You have completed this procedure.

Creating an SNMP User Using CTC

Purpose	This procedure enables you to create a SNMP user.
Tools/Equipment	None

Prerequisite Procedures	• "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* • Create Group Access Using CTC, on page 163
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **Users** tabs.

Step 2 Click **Create**.

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

- User Name— Specify the name of the user on the host that connects to the agent. The user name must be a minimum of 6 and a maximum of 40 characters (up to only 39 characters for the TACACS and RADIUS authentication). It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, "-" (hyphen), and "." (dot) . For TL1 compatibility, the user name must be of 6 to 10 characters.
- Group Name—Specify the group to which the user belongs.
- The SNMP version and security level of the group are displayed as read-only.
- Owner—Specify the user access. The values are:
  - **None**
  - **SDROwner**: Limits access to owner service domain router (SDR).
  - **SystemOwner**: Provides system-wide access including access to all non-owner SDRs.
- Authentication
  - Protocol—Select the authentication algorithm that you want to use. The options are None, MD5, and SHA.
  - Password—Enter a password if you select MD5 or SHA. By default, the password length is set to a minimum of eight characters.

  Note This field is enabled only when SNMP version of the Group is SNMPV3 and Security Level of the group is authNoPriv or authPriv.

- Privacy—Initiates a privacy authentication level setting session that enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select the privacy authentication algorithm. The available options are None, DES,3DES,AES128,AES192 and AES256.
  - Password—Enter a password if you select a protocol other than None.

Note This field is enabled only when SNMP version of the Group is SNMPV3 and Security Level of the group is authPriv.

Step 4 Click **OK** to create an SNMP user.

Stop. You have completed this procedure.

Create MIB Views Using CTC

Purpose	This procedure enables you to create SNMP MIB view.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **MIB views** tabs.

Step 2 Click **Create**.

Step 3 In the Create Views dialog box, enter the following information:

- Name—Name of the view.
- Subtree OID—The MIB subtree which, when combined with the mask, defines the family of subtrees.
- Type—Select the view type. Options are Included and Excluded.

  Type defines whether the family of subtrees that are defined by the subtree OID and the bit mask combination are included or excluded from the notification filter.

Step 4 Click **OK** to save the information.

Stop. You have completed this procedure.

Configure SNMP Trap Destination Using CTC

Purpose	This procedure enables you to configure SNMP trap destination.

Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **Trap Destinations** tabs.

Step 2 Click **Create**.

Step 3 In the Create SNMP Trap dialog box, enter the IP address of your network management system (NMS).

Step 4 Click **OK** to save the information.

Stop. You have completed this procedure.

Create SNMP Community Using CTC

Purpose	This procedure enables you to create SNMP community.
Tools/Equipment	None
Prerequisite Procedures	• "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* • Creating an SNMP User Using CTC, on page 164 • Configure SNMP Trap Destination Using CTC, on page 166
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **Trap Destinations** tabs.

Step 2 In the Communities area, click **Create**.

The Create SNMP Community dialog box appears.

Step 3 In the Destination area, the Destination Address field displays the trap destination address configured in Configure SNMP Trap Destination Using CTC, on page 166.

Step 4 Enter the User Datagram Protocol (UDP) port on which you want to create a community in the UDP Port field.

The default UDP port for SNMP is 162.

Step 5 In the User area, choose the user from the User Name droop-down list.

The SNMP version and the security level of the selected user are displayed.

Step 6 In the Notification area, check the required basic trap types. The available options are BGP, Config, Syslog, and SNMP.

Step 7 From the Advance Trap Types drop-down list, choose **None** or **Copy Complete**.

Step 8 Click **OK** to create SNMP community.

Stop. You have completed this procedure.

Enabling SNMP Trap Notifications Using CTC

Purpose	This procedure enables SNMP trap notifications that are sent to a MIB tree.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP** > **Notifications** tabs.

Step 2 In the Notifications area, enable the following notifications as required by checking the **Enable** check box next to each notification.

- BGP—Border Gateway Protocol (BGP) trap notifications
- Config—Configuration trap notifications
- SNMP—SNMP trap notifications
- Syslog—Trap notifications in the system log file

Step 3 Click **Apply**.

Stop. You have completed this procedure.

Manually Configuring the SNMPv3 Proxy Forwarder Table

Purpose	This procedure enables you to create an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In network view, click **Provisioning** > **SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- From the GNE drop-down list, choose the GNE to be used as the SNMPv3 proxy server.
- Check the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Manual Create**.

Step 4 In the Manual Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Proxy Type—Select the type of SNMP request that needs to be forwarded. The options are Read and Write.
- Target Address—Target to which the request should be forwarded. Select from drop down list, an IPv4 or an IPv6 address.
- Context Engine ID—The context engine ID of the ENE to which the request is to be forwarded. The context engine ID should be the same as the context engine ID of the incoming request.
- Local User Details—The details of the local user who proxies on behalf of the ENE user.
  - User Name—Select the name of the user on the host that connects to the agent.
  - Local Security Level—Select the security level of the incoming requests that are to be forwarded. The options are noAuthNoPriv, authNoPriv, and authPriv.
- Remote User Details—The details of the remote user to which the request is forwarded.
  - User Name—Select the user name of the remote user.

- Remote Security Level—Select the security level of the outgoing requests. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Authentication
    - Protocol—Select the authentication algorithm you want to use. The options are None, MD5, and SHA.
    - Password—Enter the password if you select MD5 or SHA.
- Privacy—Enables the host to encrypt the contents of the message that is sent to the agent.
    - Protocol—Select NONE ,DES or AES-256-CFB as the privacy authentication algorithm.
    - Password—Enter the password if you select protocol other than None. The password should not exceed 64 characters.

Step 5 Click **OK** to save the information.

Stop. You have completed this procedure.

Automatically Configuring the SNMPv3 Proxy Forwarder Table

Purpose	This procedure enables you to create an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In network view, click **Provisioning** > **SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- From the GNE drop-down list, choose the GNE to be used as the SNMPv3 proxy server.
- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Proxy Type—Select the type of proxies to be forwarded. The options are Read and Write.
- Security Level—Select the security level for the incoming requests that are to be forwarded. The options are:
    - noAuthNoPriv—Uses a username match for authentication.
    - authNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
    - authPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.
- Local User Name—Select the user name from the list of users.
- Target Address List—Select the proxy destination.

Note When you configure SNMPv3 Proxy Forwarder Table automatically, the default_group is used on the ENE. The default_group does not have write access. To enable write access and allow SNMP sets, you need to edit the default_group on ENE.

Step 5 Click **OK** to save the settings.

Step 6 Return to your originating procedure.

Automatically Configuring the SNMPv3 Proxy Trap Forwarder Table

Purpose	This procedure enables you to create an entry in the SNMPv3 Proxy Trap Forwarder Table automatically.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In network view, click **Provisioning** > **SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- From the GNE drop-down list, choose the GNE to be used as the SNMPv3 proxy server.

- Check the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the **SNMPv3 Proxy Trap Forwarder Table** area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Trap Forwarder dialog box, enter the following information:

- Target Tag—Specify the tag name. The tag identifies the list of NMS that should receive the forwarded traps. All GNE Trap destinations that have this tag in their proxy tags list are chosen.
- Remote Trap Source List—The list of ENEs whose traps are forwarded to the SNMPv3 Trap destinations that are identified by the Target Tag.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure.

CHAPTER 16

Upgrade a Fabric Card

This chapter describes the procedure to upgrade the NCS4009-FC2-S fabric card to the NCS4009-FC2F-S fabric card.

Upgrading a Fabric Card

Purpose	This procedure provides instructions for upgrading from a NCS4009-FC2-S fabric card to a NCS4009-FC2F-S fabric card.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Maintenance** tab.

Step 2 Click **Fabric Upgrade** to get the current Fabric Details. The table displays the following details:

Title	Description
Plane ID	Displays all the plane IDs.
Plane Admin Status	Displays current admin status of all planes. The admin status can either be Up or Down.
Plane Oper Status	Displays current operational status of all planes. The operational status can either be Up or Down.
Hardware Status	Displays hardware status of all Fabrics. The possible states are IS-NR and OOS-AU, indicating In-service and Out-of-service, respectively.

Title	Description
Product ID	Displays the Product ID of all fabrics. Before upgrade, the displayed product ID is NCS4009-FC2-S.

Note The Plane Admin status and the Plane Oper status need to be Up for all the Plane IDs before proceeding with the fabric card upgrade.

The Fabric Details table is for display purpose only, the displayed elements cannot be selected.

Step 3 In the **Upgrade Wizard** pane, select the fabric plane from the **Available Fabrics** drop-down menu.

Step 4 Click **Next** to shutdown the selected fabric plane; this is indicated as Step 1.

The **Available Fabrics** option is grayed-out until the upgrade process for the selected fabric card is complete.

From this step onwards, we shall refer to the right side of the **Upgrade Wizard** pane, where the steps are discussed for the fabric card upgrade.

Step 5 Click **Yes** on the **Confimation Dialog** .

A message is displayed indicating that the selected plane was successfully shutdown.

Step 6 Click **Next** to shutdown the selected fabric card; this is indicated as Step 2.

Check the Plane Admin Status, Plane Oper Status and Hardware Status in the Fabric Details pane. They will be displayed as Down, Down, OOS, DSBLD respectively.

Click **Revert** if you do not wish to proceed with the upgrade and unshut the plane.

Step 7 Remove the NCS4009-FC2-S fabric card.

Step 8 Install the NCS4009-FC2F-S fabric card and the auxiliary fan tray (NCS4009-FAN-FC).

Step 9 Click **Next**. This is indicated as Step 3.

Click **Revert** if you do not wish to proceed with the upgrade and unshut the fabric card. Do not use this option after manually replacing the fabric card.

Step 10 Wait for the Hardware Status column, in the Fabric Details pane, to display the current status of the fabric card and click **Next**. This is indicated as Step 4.

The Hardware Status is now displayed as IS-NR, IS-NR and both the PIDs (fabric card and the auxiliary fan tray) are displayed in the Product ID column. This may take a few minutes.

Step 11 Click **Next** to upgrade all FPDs of the selected fabric. This is indicated as Step 5.

Step 12 On choosing to upgrade the FPD device, a message is displayed recommending the user to check the FPD status under the **Maintenance** > **Software** > **FPD Upgrade** tab.

The user has an option to click **Skip** to proceed without upgrading the FPD devices. The user can revisit the **FPD Upgrade** tab anytime to upgrade the FPDs. The user can choose to skip the FPD upgrade if the new cards have their FPD images already aligned.

Step 13 Check the current status of the newly installed FC. Reload the FC if the current status is indicated as *Reload required*.

Step 14 Click **Finish**, to activate (no shutdown) the fabric plane. This is indicated as Step 6.

Check the Plane Admin Status, Plane Oper Status and Hardware Status. They will be displayed as Up, Up, IS-NR, IS-NR respectively.

The **Available Fabrics** drop-down menu is now available, wherein the user can select another fabric card.

What to do next

After all the fabric cards are upgraded to the NCS4009-FC2F-S fabric card, the air filter needs to be replaced. The NCS4009-FC2F-S fabric card supports Cisco PID NCS4009-FTF-2.

CHAPTER 17

Cable Management Utility

This appendix describes the cable management uility in CTC that helps you with the cabling process between the fabric cards of the LCC and FCC in a multi-chassis configuration.

Cable Management Utility

The cable management wizard can be used to make CXP connections between the fabric cards of the FCCs and LCCs. The CXP connections are color coded.

- Green: The ports are green when they are connected properly.
- Red: The ports are red when the plane is shut down or the ports are incorrectly connected.

The following pre-requisites must be completed before the cable management process can start:

- Cabling of the ethernet control connections between the RP cards of the LCC and the RPMC cards of the FCC must be completed. For more information, see the *Cisco Network Convergence System 4000 Fabric Card Chassis Hardware Installation Guide*.
- When the system is up, the instance configuration must be completed. For more information, see the *Cisco Network Convergence System 4000 Fabric Card Chassis Hardware Installation Guide*.
- The plane must be shut before starting the cabling process. To shut the plane, perform the following steps:
  1. Go to the CTC multi-shelf view > Fabric Plane tab.
  2. Click Fabric Plane Maintenance.

     The Fabric Plane Maintenance window opens.
  3. Select the plane from the Plane ID drop-down list and choose the OOS, DSBLD option from the Admin State drop-down list.
  4. Click Apply.

The cable management wizard can be started by either clicking the Cable Management button in the CTC multi-shelf view > Provisioning > General >Rack Management tab or by clicking the Cable Management icon in the toolbar.

The wizard has two configuration views:

- LCC connections:This view displays one LCC at a time. You can select the LCC to view from the drop-down list.
- Plane connections: This view displays the fabric cards that are configured in a specific plane. You can select the plane to view from the drop-down list.

The Cable Management window consists of:

- Graphical View: This pane allows you to view all the cable management related information in the LCC or Plane Connections view. The cable management process can also be started by either selecting any unconnected port or by clicking the Start button in this view. The ports to be connected start blinking after the cable management process has begun.
- Actions tab: This tab displays context aware actions and information. When the cable management process is started, this tab displays a table that consists of a group of port pairs that need to be connected. Textual information on which ports need to be connected is displayed on the right. When the user connects the cable and clicks on Next, the connection is validated. If the connection is correct, then the blinking moves onto the next port that is to be connected. A warning message is displayed if the connection is down. Click Yes to skip this row and move to the next.
- Connections Table tab: This tab displays all the ports that need to be connected and their connection status in a tabular format. This information can be exported to a file in HTML, CSV, or TSV format or printed for offline access.

After all the ports have been connected, you need to unshut the plane. To unshut the plane, perform the following steps:

1. Go to the CTC multi-shelf view > Fabric Plane tab.
2. Click Fabric Plane Maintenance.

   The Fabric Plane Maintenance window opens.
3. Select the plane from the Plane ID drop-down list and choose the IS option from the Admin State drop-down list.
4. Click Apply.

The connection status in the Connection Table displays connected.

For information about troubleshooting the fabric cable connections, see the *Single Chassis to Multi-Chassis MOP*.

CHAPTER 18

Configure Affinity for OTN using CTC

This chapter describes the CTC procedure for configuring Affinity Support for OTN GMPLS.

Affinity for OTN GMPLS Overview

The Affinity Support for OTN GMPLS feature steers the selection of paths for MPLS TE tunnel, adhering to affinity constraints.

Affinity can be configured through CTC or CLI using following steps :

- Define affinity map, which is a global name-to-value mapping. Here name is a colour and value is a bit value (0-31). This mapping is used to assign colour(s) to TE link.

Note Same bit position should not be used for more than one colour in the map.

- Assign a TE link with one or multiple colours.
- Create attribute-set(affinity profile) that defines affinity constraints. These constraints are used for circuit path calculation.
- Assign attribute set(s) to an OTN tunnel.

Note Affinity mapping bit should be same in all over network.

Configuring Affinity for GMPLS using Cisco IOS XR commands

Procedure

Step 1 Define colours and assign bits to each colour using command : **affinity-map** *<colour>* **bit-position** *<bit position>*

Example:

```
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-mpls-te)# affinity-map green bit-position 0
```

Note Only one colour can be mapped to a particular bit position.

Note Same bit map should defined at all the connected nodes.

Step 2 Assign one or multiple colours to the OTN link using command **affinity-name***<colour>*

Example:

```
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
```

Note Assign colour to all the ports of the connected nodes.

Step 3 Define an attribute set using command **attribute-set path-option**

This will define the affinity constraints.

Example:

```
RP/0/RP0:hostname# configure terminal
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
```

Step 4 Configure **attribute-set** for **path–option** for OTN tunnel.

This will assign affinity constraints to OTN tunnel. Following are the constraint type:

- **include** : 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** : 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**: 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.

  Note In case of exclude-all constraint, other configured constraints for the same tunnel will be ignored.

Example:

```
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 7
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)# signalled-bandwidth ODU2
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)# destination ipv4 unicast 192.168.0.3
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)# path-option 1 dynamic attribute-set Affinity1
protected-by 2 restored-from 3 lockdown
RP/0/RP0:hostnam (config-te-gmpls-tun-0x7)# path-option 2 dynamic attribute-set Affinity2
lockdown
```

Step 5 Verify the configurations using show commands.

Example:

```
RP/0/RP0:hostname# show mpls traffic-eng affinity-map

Tue Jun 26 15:12:01.948 IST
                      Affinity Name     Bit-position            Affinity Value
Affinity Table
  ----------------------------------   --------------        -----------------------
----------------
                                red                2           0x::4
Mapping
                             yellow                3           0x::8
Mapping
                               blue               21           0x::20:0
Mapping
                              green               31           0x::8000:0
Mapping

RP/0/RP0:hostname# show mpls traffic-eng link-management optical-nni controller otu2 0/0/0/22

Tue Nov  7 11:52:51.063 IST
System Information::
NNI OTN Links Count: 3 (Maximum NNI OTN Links Supported 300)
Link Name:: OTU20_0_0_22 (Handle:0x00000170, Addr: V4-Unnum 192.168.0.1 [17])
Link Status         : Up
Link Label Type     : G709_ODU
Physical BW         : OTU2 (10.709Gbps)
Max LSP Bandwidth Per Priority(kbps):
  Priority[0] : 7495557
  Priority[1] : 0
  Priority[2] : 0
  Priority[3] : 0
  Priority[4] : 0
  Priority[5] : 0
  Priority[6] : 0
  Priority[7] : 0
Fixed ODU Capabilities:
     Signal Type       Stages            Flags             Resources
                   1   2   3   4   T S 1.25G 2.5G V L Maximum    Unreserved
                   -   -   -   -   - - ----- ---- - - -------    ----------
   ODU2                            Y Y Y     N    N N 1          0
   ODU0            2               Y Y Y     N    N N 8          6
   ODU1            2               Y Y Y     N    N N 4          3
Flex  ODU Capabilities:
     Signal Type       Stages            Flags              Bandwidth(kbps)
                   1   2   3   4   T S 1.25G 2.5G V L Maximum   Unreserved  Max Lsp
                   -   -   -   -   - - ----- ---- - - --------  ----------  --------
   ODUFlex CBR     2               Y Y Y     N    N N 9995277   7495557     7495557
   ODUFlex GFPFix  2               Y Y Y     N    N N 9995277   7494313     7494313

SRLG Values:1,
TTI Mode            : Section Monitoring
TCM ID              : 0
IGP Neighbor Count  : 1
Flooding Status: (1 area)
IGP Area[1]:: OSPF, ring, 0: Flooded
Remote Link Id:V4-Unnum 192.168.0.2 [16], TE Metric: 1
Delay(Configured/Computed/ToFlood): 0/0/300000 micro-sec
Attributes          :  0x2
Attribute Names     :  red(1)
```

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

IGP Id: 192.168.0.4, MPLS TE Id: 192.168.0.4 Router Node  (OSPF ring area 0)
  Link[0]:Point-to-Point, Nbr IGP Id:192.168.0.2, Nbr Node Id:2, gen:28399
      Attribute Flags: 0x2
      Ext Admin Group:
          Length: 256 bits
          Value : 0x::2
     Attribute Names: red(1)
      Intf Id:13 Nbr Intf Id:15 TE Metric:1
      Uni Delay:300000
      SRLGs: 3
      Switching Capability:otn, Encoding:g709-otn
      Physical BW:10709224 (kbps), Max Reservable BW:10709224 (kbps)
      Max LSP Bandwidth Per Priority(kbps):
        Priority[0] : 7495556
        Priority[1] : 0
        Priority[2] : 0
        Priority[3] : 0
        Priority[4] : 0
        Priority[5] : 0
        Priority[6] : 0
        Priority[7] : 0
      Fixed ODU Capabilities:
           Signal Type       Stages            Flags             Resources
                         1   2   3   4   T S 1.25G 2.5G V L Maximum    Unreserved
                         -   -   -   -   - - ----- ---- - - -------    ----------
         ODU2                            Y Y Y     N    N N 1          0
         ODU0            2               Y Y Y     N    N N 8          6
         ODU1            2               Y Y Y     N    N N 4          3
      Flex  ODU Capabilities:
           Signal Type       Stages            Flags               Bandwidth(kbps)

                         1   2   3   4   T S 1.25G 2.5G V L Maximum   Unreserved  Max Lsp

                         -   -   -   -   - - ----- ---- - - --------  ----------  --------

         ODUFlex CBR     2               Y Y Y     N    N N 9995277   7495556     7495556

         ODUFlex GFPFix  2               Y Y Y     N    N N 9995277   7494312     7494312
```

```
RP/0/RP0:hostname# show mpls traffic-eng attribute-set path-option test2

Thu Dec 21 14:12:43.364 IST
Attribute Set Name: test2 (Type: path option)
  Bandwidth: 0 kbps (CT0) (Default)
  Number of affinity constraints: 3
     Include bit map           : 0x2
     Include ext bit map       :
         Length: 256 bits
         Value : 0x::2
     Include affinity name     : red(1)
     Include bit map           : 0x4
     Include ext bit map       :
         Length: 256 bits
         Value : 0x::4
     Include affinity name     : blue(2)
     Include bit map           : 0x8
     Include ext bit map       :
         Length: 256 bits
         Value : 0x::8
     Include affinity name     : yellow(3)
  Exclude List Name:  none (Default)
  List of tunnel IDs (count 0)
```

```
RP/0/RP0:hostname# show mpls traffic-eng tunnels 7 detail

Tue Nov  7 11:19:28.610 IST
Name: Odu-Group-Te7  Destination: 192.168.0.4  Ifhandle:0xd0
  Signalled-Name: rtrA_otn7
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected
    path option 1, (LOCKDOWN) type dynamic  (Basis for Current, path weight 2)
      Protected-by PO index: none
      Path-option attribute: test_red
        Number of affinity constraints: 1
          Include bit map           : 0x2
           Include ext bit map       :
               Length: 256 bits
               Value : 0x::2
           Include affinity name     : red(1)
        Reroute pending (DROP)
    path option 2, (LOCKDOWN) type dynamic
      Path-option attribute: test_red
        Number of affinity constraints: 1
           Include bit map           : 0x2
           Include ext bit map       :
               Length: 256 bits
               Value : 0x::2
           Include affinity name     : red(1)

    Last PCALC Error [Standby]: Mon Nov  6 16:52:34 2017
      Info: No diverse path found
    Bandwidth Requested: 2498775 kbps  CT0
    Creation Time: Mon Nov  6 15:36:06 2017 (19:43:22 ago)
  Config Parameters:
    Bandwidth: ODU1
    Priority: 24  0 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    Path Selection:
      Tiebreaker: Min-fill (default)
    Hop-limit: disabled
    Cost-limit: disabled
```

```
   Delay-limit: disabled
   Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
   AutoRoute: disabled  LockDown:  enabled  Policy class: not set
   Forward class: 0 (not enabled)
   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: 13
 Binding SID: None
 Path Protection Info:
   SNC Mode:SNC-N , TCM id: Not used , Type:Bi-directional APS, Non-revertive
   Restoration style: keep-failed-lsp
   Path Protection Profile Type: 1+0
   Timers WTR: 300000 milliseconds, HoldOff: 0 milliseconds
   Active Lsp: WORKING LSP, Standby Diversity Type: None
 Restoration Info:
   Non-revertive
   Diverse Lsp for UNKNOWN, Diversity Type: None
 Revert Schedule: Not Configured
 Static-uni Info:
   Locally Client Port:   Client Ifhandle: 0x0
   Client ODU:   Client ODU Ifhandle: 0x0
     XC Id: 0
     State: Not Connected
     Uptime: Thu Jan  1 05:30:00 1970
 Working Homepath ERO:
   Status: Down
   Explicit Route:
 Diversity Info:
   Dependent Tunnel List:
      8

 Current LSP Info:
   Instance: 2108, Signaling Area: OSPF ring area 0
   Uptime: 18:27:10 (since Mon Nov 06 16:52:18 IST 2017), Signaling State: Up, Oper State:
Up
   G-PID: None (0)
     XC Id: 0
     State: Connected
     Uptime: Mon Nov  6 16:52:18 2017
     Egress Interface: OTU20/0/0/22 (State:Up  Ifhandle:0x170)
     Egress Controller: ODU20_0_0_22 (State:Up Ifhandle:0x190)
     Egress Sub Controller: ODU10_0_0_22_41 (State:Up, Ifhandle:0x3d0)
     Path Ingress  label: TPN: 4 BitMap Len: 8 BitMap: 7:8
     Resv Egress  label: TPN: 4 BitMap Len: 8 BitMap: 7:8
   Router-IDs: local      192.168.0.1
               downstream 192.168.0.2
   Soft Preemption: None
   SRLGs: not collected
   Path Info:
     Outgoing:
       Explicit Route:
         Strict, 192.168.0.2(16)
         Strict, 192.168.0.4(13)
         Strict, 192.168.0.4

     Record Route: Empty
     Tspec: signal_type ODU1 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 192.168.0.2, flags 0x20 (Node-ID)
        Label          Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1

        Unnumbered 192.168.0.2 (16), flags 0x0
        Label          Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1
        IPv4 192.168.0.4, flags 0x20 (Node-ID)
        Label          Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1

        Unnumbered 192.168.0.4 (13), flags 0x0
        Label          Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1
      Fspec: signal_type ODU1 Bitrate 0kbps NVC 0 MT 1

  Persistent Forwarding Statistics:
    Out Bytes: 0
    Out Packets: 0
Displayed 1 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Configuring Affinity Using CTC

Purpose	This procedure enables you to configure an OTN tunnel with path adhering to affinity constraints, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 To define affinity map, complete Define Affinity Map Using CTC, on page 186

Step 2 To assign OTN link with one or multiple colours, complete Assign Affinity Name(s) to TE Link Using CTC, on page 186

Step 3 To create affinity profile defining affinity constraints, complete Define Affinity Profile Using CTC, on page 187

Step 4 To assign affinity profile(constraints) to OTN tunnel, complete Configure an OTN Circuit Using CTC, on page 84.

Stop. You have completed this procedure.

Define Affinity Map Using CTC

Purpose	This procedure enables you to define affinity names(colours) and assign bits to each affinity name, using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the OTN > Affinity > Affinity Mapping tabs.

Step 2 Click the **Add Mapping** button.

Step 3 In the Add Mapping dialog box, enter the following :

- Affinity Name - Enter the colour.
- Bit Value - Select the bit value corresponding to the affinity name(colour).

Step 4 Select an affinity mapping and click **Store** button.

Step 5 In the Affinity Mapping Storing dialog box, select the node to save the affinity mapping.

Step 6 Click **ok** to save the selected affinity mapping on the selected node in the network .

You can use the **Load** button to verify if the affinity map is sucessfully saved.

Step 7 Return to your originating procedure.

Assign Affinity Name(s) to TE Link Using CTC

Purpose	This procedure enables you to assign an OTN link with one or multiple affinity names(colours), using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, click the Provisioning > Network > MPLS-TE tabs.

Step 2 In the Controllers section, select a line card and expand the corresponding section to see the list of controllers.

Step 3 To update the affinity name for the controller, double click the **Affinity Name** column.

Step 4 In the dialog box, select one or multiple affinity names(colours) and click **Ok**.

This will assign affinity name(s) to the selected controller(TE link).

Note A TE link can be assigned maximum of 32 colours.

Note Assign same affinity name(colour) for the controlleres on both source and destination end of the TE link.

Step 5 Return to your originating procedure.

Define Affinity Profile Using CTC

Purpose	This procedure enables you to define affinity constraints to be used for circuit path calculation.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the OTN > Affinity > Affinity Profile tabs.

Step 2 Click the **Create** button.

Step 3 In the Create Affinity Profile dialog box:

- Name - Enter name of Affinity Profile(Affinity Constraint).
- Node Name - Select the node on which you want to save the profile.
- Constraint Type - Select the constarint type from the drop down list.

Following are the constraint types:

- **include** : 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** : 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**: 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.

  Note In case of exclude-all constraint, other configured constraints for the same tunnel will be ignored.

- Affinity Names - Select one or multiple affinity names(colours).

  Note Each constraint can have maximum 10 colours.

- Add Constarint - Click **Add Constraint** button, to add the constraint to the affinity profile.

Step 4 Click **Apply** button, to save the affinity profile.

Step 5 Return to your originating procedure.

CHAPTER 19

Migration : NCS4K-ECU to NCS4K-ECU2

This chapter provides the CTC procedure for migration of Extenal Connection Unit (ECU) in a Multi Chassis system.

Migrate from NCS4K-ECU to NCS4K-ECU2

Purpose	This procedure provide instructions to migrate from NCS4K-ECU to NCS4K-ECU2 using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Do not perform router or route processor reload during the migration procedure.

Note To check the current status of migration while performing this procedure, click the **Status** button.

Note You can check the alarm(s) and alarm state in the **Alarms** tab of CTC.

Procedure

Step 1 In the **Node View**, click the **Maintenance** > **ECU Upgrade** tab.

Step 2 Click the **Detach** button.

Step 3 Click the **Yes** button.

Alarms **The Detach Operation for disk started** and **Disk provision** will be raised.

Step 4 Wait for the alarm **The Detach Operation for disk started** to clear.

Note The **Disk provision** alarm will persist all through the migration procedure.

Step 5 Remove the NCS4K-ECU unit physically form the chassis and replace it with the NCS4K-ECU2 unit.

Note For detailed procedure on Removing and Replacing the ECU unit refer *Hardware Installation Guide for Cisco NCS 4000 Series*.

Step 6 Wait 2-3 minutes, for the newly installed ECU unit to initialize.

Step 7 Check to ensure that the **ECU Plugged out** alarm has cleared.

Note Proceeding to next step without waiting for ECU Plugged out alarm to clear, may lead system to inconsistent system state.

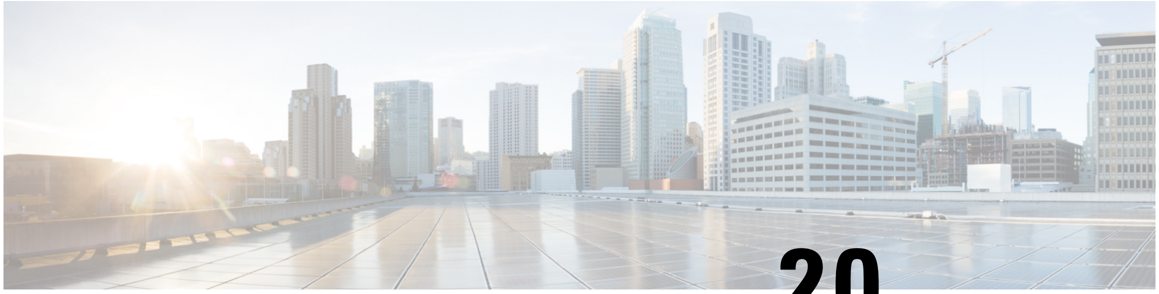
Step 8 Click the **Attach** button.

This will trigger the attach procedure and **The attach provision for disk started** alarm will be raised.

Step 9 Wait for **Disk Provision** and **The attach provision for disk started** alarms to clear.

Once above alarms are cleared from the system, ECU migration from NCS4K-ECU to NCS4K- ECU2 is completed successfully.

Stop. You have completed this procedure.



CHAPTER 20

24 Low Rate (LR) Datapath

This chapter provides conceptual information about 24 LR datapath feature on Cisco NCS 4000 Series routers.

Overview

To handle low rate client signal on NCS4K, this feature provides low rate (OC3/OC12/STM1/STM4) data path support on NCS4K-24LR-O-S line card.

Following are the characteristics limitations of this feature:

- Packet fuctionalities are not supported.
- Only single TCM functionality is supported.
- PRBS is not supported.
- Loopback is not supported on cross connected ODU.
- NCS4K-24LR-O-S line card has maximum 40G capacity. There are four10G port and 20 low rate ports. Since at a time we cannot use all ports below are few combinations which can be used:
    - On ports 0 to 3, OC3/OC12 can be allocated only if 10GE/OC192 traffic is not configured on Port 22; on port 4 OC3/OC12 can be allocated only if OC48 is not configured on port 0; on port 22 OC3/OC12 can be allocated only if OC48 is not configured on port 2.
    - On ports 6 to 9, OC3/OC12 can be allocated only if 10GE/OC192 traffic is not configured on Port 10; on port 5 OC3/OC12 can be allocated only if OC48 is not configured on port 6; on port 10 OC3/OC12 can be allocated only if OC48 is not configured on port 8.
    - On ports 12 to15, OC3/OC12 can be allocated only if 10GE/OC192 traffic is not configured on Port 23; on port 16 OC3/OC12 can be allocated only if OC48 is not configured on port 12; on port 23 OC3/OC12 can be allocated only if OC48 is not configured on port 14.
    - On ports 18 to 21, OC3/OC12 can be allocated only if 10GE/OC192 traffic is not configured on Port 11; on port 17 OC3/OC12 can be allocated only if OC48 is not configured on port 18; on port 11 OC3/OC12 can be allocated only if OC48 is not configured on port 20.

CHAPTER 21

Configure Link Layer Discovery Protocol Using CTC

Table 16: Feature History

Feature Name	Release Information	Description
Link Layer Discovery Protocol (LLDP) on NCS4K-4H-OPW-QC2 line card	Cisco IOS XR Release 6.5.33	In addition to the existing support on packet interfaces, Link Layer Discovery Protocol (LLDP) is now enabled on the client ports of the NCS4K-4H-OPW-QC2 card that carry Ethernet-over-OTN traffic. This feature allows NCS 4000 to discover peer devices connected either on the OTN ports or the packet interfaces. As a result, it reduces the need to use multiple protocols for network management, especially in a multi-vendor network.

Link Layer Discovery Protocol for Ethernet-over-OTN

LLDP is a link layer protocol that allows NCS 4000 devices to transmit and receive device information from its neighbor devices connected through the client ports 0 to 9 that support Ethernet over OTN configuration and the package interfaces of the NCS4K-4H-OPW-QC2 line card.

Some of the details that can be sent and gathered by NCS 4000 if LLDP is enabled are:

- System name and description
- Port name and description
- MAC address and IP address

- Capabilities of the device

Enable LLDP on NCS4K-4H-OPW-QC2 Card using CTC

Purpose	This procedure describes how to enable LLDP on NCS 4000 using CTC that allows to learn the information of its peer devices connected through the Ethernet over OTN port.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Software Installation Guide for Cisco NCS 4000 Series
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click **Provisioning** > **Network** > **LLDP**.

Step 2 Select the **LLDP** check box.

Step 3 Click **Apply**.

View Neighbor Device Details Using CTC

Purpose	This procedure enables you to view the details of the neighbor devices connected to NCS 4000 through the Ethernet over the OTN port using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Software Installation Guide for Cisco NCS 4000 Series
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click **Maintenance** > **Network** > **LLDP**.

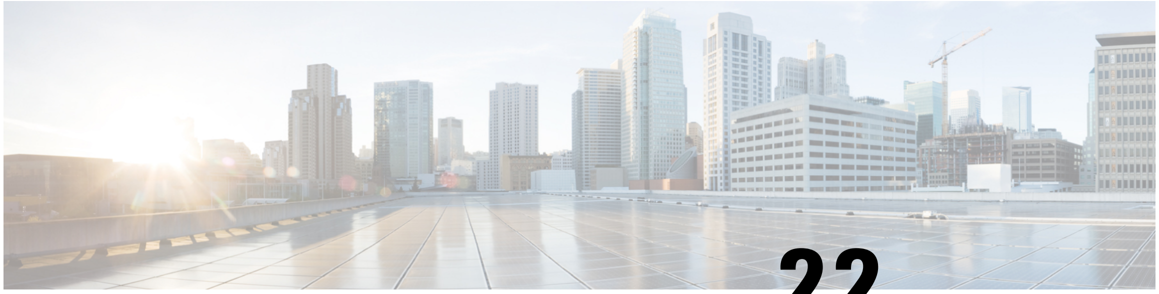
Step 2 Perform one of the following:

a) Click the **Neighbor** tab to view neighbor devices.
b) Click the **Neighbor Details** tab to view details of the neighbor devices.

Step 3 Click **Refresh** to refresh all the details in the tab.

PART II

Configurations Using IOS XR



CHAPTER 22

Configure Authentication

This chapter describes the procedures to configure the authentication and multiple privilege levels. It describes the procedures to encrypt a password and change the static or line password. This chapter also explains to manage the RADIUS and TACACS server.

Change a Static Enable Password

Perform this task to change the Static Enable password.

Procedure

Step 1 **configure**

Step 2 **username** *name-of-the-user*

Example:

```
RP/0/RP0:hostname (config)# username user1
```

Enters the user name mode.

Step 3 **password** *text.*

Example:

```
RP/0/RP0:hostname (config-un)# password pwd1
```

Enters the password.

Step 4 **commit**

Change a Line Password

Perform this task to change the line password.

Procedure

Step 1 **configure**

Step 2 **username** *name-of-the-user*

Example:

```
RP/0/RP0:hostname (config)# username user1
```

Enters the user name mode.

Step 3 **password** *text*

Example:

```
RP/0/RP0:hostname (config-un)# password pwd1
```

Enters the password.

Step 4 **commit**

Encrypt Password

Perform this task to encrypt the password.

Procedure

Step 1 **configure**

Step 2 **username** *name-of-the-user*

Example:

```
RP/0/RP0:hostname (config)# username user1
```

Enters the user name mode.

Step 3 **encrypt password** *text*

Example:

```
RP/0/RP0:hostname (config-un)# password 7 pwd1
```

Encrypts password.

Step 4 **commit**

Configure Privilege Levels

Before you begin

Optics controller should be created before configuring the privilege levels.

Procedure

Step 1 **configure**

Step 2 **username** *name-of-the-user*

Example:

```
RP/0/RP0:hostname (config)# username user1
```

Enters the user name mode.

Step 3 **privilege level**

Example:

```
RP/0/RP0:hostname (config-un)user group 2
```

Configures the privilege level.

Step 4 **commit**

Manage RADIUS Server

Perform this task to manage the radius server.

Procedure

Step 1 **configure**

Step 2 **username** *name-of-the-user*

Example:

```
RP/0/RP0:hostname (config)# username user1
```

Enters the user name mode.

Step 3 **aaa new-model**

Example:

```
RP/0/RP0:hostname (config)# aaa new-model
```

Adds a new model.

Step 4 **radius-server host** *IP-address* **auth-port** *port-number* **acct-port** *port-number* **key** *name*

Example:

```
RP/0/RP0:hostname (config)# radius-server host 10.78.161.120 auth-port 1812 acct-port 1813
 key SECRET_KEY
```

Adds a radius server.

Step 5 **aaa authentication**

Example:

```
RP/0/RP0:hostname (config)# aaa authentication login default group radius local
```

Adds AAA authentication.

Step 6 **aaa authorization**

Example:

```
RP/0/RP0:hostname (config)# aaa authorization exec default group radius if-authenticated
```

Adds AAA authorization.

Step 7 **aaa accounting**

Example:

```
RP/0/RP0:hostname (config)# aaa accounting exec default start-stop group radius
```

Adds AAA accounting.

Step 8 **commit**

Manage TACACS Server

Perform this task to manage the TACACS server.

Procedure

Step 1 **configure**

Step 2 **username** *name-of-the-user*

Example:

```
RP/0/RP0:hostname (config)# username user1
```

Enters the user name mode.

Step 3 **aaa new-model**

Example:

```
RP/0/RP0:hostname (config)# aaa new-model
```

Adds a new model.

Step 4 **aaa authentication**

Example:

```
RP/0/RP0:hostname (config)# aaa authentication login default group tacacs+ local
```

Adds AAA authentication.

Step 5 **tacacs-server host** *IP-address*

Example:

```
RP/0/RP0:hostname (config)# tacacs-server host 10.78.161.120
```

Adds a TACACS server host.

Step 6 **tacacs-server key** *name*

Example:

```
RP/0/RP0:hostname (config)# tacacs-server key otntest
```

Adds a TACACS server key.

Step 7 **commit**

AAA Password Security Policies

Table 17: Feature History

Feature Name	Release Information	Description
AAA Password Security Policies	Cisco IOS XR Release 6.5.33	This feature introduces strong password security policies to strengthen the secret and password configuration of usernames. These policies also have the option of blocking a local user from accessing the router for a configurable amount of time if the maximum number of attempts to login to the device is reached. The feature thus enhances router security by enforcing strong user password policies. Commands added: • policy

The AAA password security policies enhance the secret configuration for the username. Currently, the password configuration in the username is supported. From the Cisco IOS-XR Release 6.5.33, the secret password policies are supported. This password policy is applicable only to local users.

AAA Password Securities have the following policies:

Lockout Policy

AAA provides a configuration option to restrict the users who try to authenticate using invalid login credentials. This option sets the maximum number of permissible authentication failure attempts for a user. The user who exceeds the maximum limit gets locked out until the configurable lockout timer is expired.

The following sample configuration specifies the maximum number of unsuccessful attempts before a user is locked out.

```
RP/0/RP1:tb6#sh run aaa password-policy pol44
aaa password-policy pol44
 lockout-time days 1
 authen-max-attempts 10
!

RP/0/RP1:tb6#
```

The following is a sample syslog when a user is locked out:

```
RP/0/RSP1/CPU0:Jun 21 09:21:28.226 : locald_DSC[308]: %SECURITY-LOCALD-5-USER_PASSWD_LOCKED
 : User 'user12’ is temporarily locked out for exceeding maximum unsuccessful logins.
This is a sample syslog when user is unlocked for authentication:
 RP/0/RSP1/CPU0:Jun 21 09:14:24.633 : locald_DSC[308]: %SECURITY-LOCALD-5-USER_PASSWD_UNLOCKED
 : User 'user12' is unlocked for authentications.
```

Lifetime Policy

The administrator can configure the maximum lifetime for the password and secret, and if this parameter isn’t set, then the password never expires.

For example, if a password has a lifetime of one month and the machine reboots on the 29th day, the password and secret is valid for one month after the reboot.

```
RP/0/RP0:R3#sh run aaa password-policy pol1
aaa password-policy pol1
 lifetime months 1
```

Reauthentication Policy

When a user attempts to log in and if the user secret credential has already expired, the user will be prompted to create a new secret.

When a user alters the secret after its lifespan expiration, the user will be authenticated against the new secret.

The following is an example showing the UI at login.

```
User Access Verification

Username: lab2
Password:

%Password has expired and must be changed.
(Requirements: Uppercase 1, Lowercase 0, Special 0,
Numeric 0, Min-length 2, Max-length 253, Min-difference 2).
Special characters restricted to !@#$%&*^()

New Password:
Confirm Password:

Password changed successfully. Please login with new password.

Username: lab2
Password:


RP/0/RP0/CPU0:ios#
```

Secret Complexity Policy

Security administrators can configure password policies to increase the complexity of the secret configuration the device. For example:

- Adding a policy to make the secret, a combination of upper and lowercase letters, numbers, and special characters.

  ```
  RP/0/RP0:R3#sh run aaa password-policy pol100
  aaa password-policy pol100
   numeric 3
   upper-case 2
   special-char 1
  !

  RP/0/RP0:R3#sh run username test_1
  username test_1
   policy pol100
   secret 5 $1$7tcr$mwCCVeDXHIy.nhzpDUSMl.
  ```

- Adding some more policies to strengthen the secret such as:
  - The maximum and minimum length of secret
  - The number of characters that must be changed in the new password compared to the old password

Enabling Secret Encryption

Table 18: Feature History

Feature Name	Release Information	Description
Stronger Secret Encryption	Cisco IOS XR Release 6.5.33	This feature introduces **secret** command that enables you to choose encryption types, such as Type 5, Type 8, Type 9, and Type 10, for encrypting the Secret. This feature employs hashing algorithms to build a more secure, strong, and robust secret to enhance the device security. Commands added: • secret

In configuring a user and group membership of that user, you can specify two types of passwords: encrypted or clear text.

The router supports both two-way and one-way (secret) encrypted user passwords. Secret is ideal for user login accounts because the original unencrypted password string cannot be deduced on the basis of the encrypted secret. Some applications (PPP, for example) require only two-way passwords because they must decrypt the stored password for their own function, such as sending the password in a packet. For a login user, both types of passwords may be configured, but a warning message is displayed if one type of password is configured while the other is already present.

If both secret and password are configured for a user, the secret takes precedence for all operations that do not require a password that can be decrypted, such as login. For applications such as PPP, the two-way encrypted password is used even if a secret is present.

Following are the different Cisco Password and Secret Types:

- **Type 5 —** Uses the Message-Digest (MD) hashing algorithms to create secret for a user.
- **Type 7 —**Uses the Vigenere cipher to create password for a user.
- **Type 8 —**Uses the Secure Hash Algorithm, 256-bits (SHA-256) to create secret for a user.
- **Type 9 —**Uses the scrypt hashing algorithm to create secret for a user.
- **Type 10 —**Uses the SHA512 algorithm to create secret for a user.

Configure Secret for Users

Each user is identified by a username that is unique across the administrative domain. Each user should be made a member of at least one user group. Deleting a user group may orphan the users associated with that group. The AAA server authenticates orphaned users, but most commands are not authorized.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:router#configure
```

Enters configuration mode.

Step 2 **username** *user-name*

Example:

```
RP/0/RP0/CPU0:router(config)#username user1
```

Creates a name for a new user (or identifies a current user) and enters username configuration submode.

Step 3 **secret{0|5|8|9|10}** *secret*

Example:

```
RP/0/RP0/CPU0:router(config-un)#secret 0 sec1
```

Specifies a password for the user named in step 2.

- Use the secret command to create a secure login password for the user names specified in step 2.
- Entering 0 followed by the password command specifies that an unencrypted (clear-text) password follows. Entering 5, 8, 9, 10 followed by the password command specifies that an encrypted password follows.

Step 4 **group** *group-name*

Example:

```
RP/0/RP0/CPU0:router(config-un)#group test
```

Step 5 Repeat step 4 for each user group the user specified in step 2 must be associated with.

Step 6 **commit**

Use the **commit** to save the configuration changes and remain within the configuration session.

Step 7 **end**

Use the **end** to take one of the following actions:

- Yes—Saves configuration changes and exits the configuration session.
- No—Exits the configuration session without committing the configuration changes.
- Cancel—Remains in the configuration session, without committing the configuration changes.

Configure Secret Type 8 and Type 9

When configuring a secret, user has the following two options:

- You can provide an already encrypted value, which is stored directly in the system without any further encryption.
- You can provide a cleartext password that is internally encrypted and stored in the system.

The Type 5, Type 8, and Type 9 encryption methods provide the above mentioned options for users to configure their passwords.

Example:

The following output is an example of directly configuring a Type 8 encrypted password:

```
RP/0/RP0/CPU0:router(config)# username demo8
RP/0/RP0/CPU0:router(confg)# secret?
RP/0/RP0/CPU0:router(config-un)#secret 8
$8$dsYGNam3K1SIJO$7nv/35M/qr6t.dVc7UY9zrJDWRVqncHub1PE9UlMQFs
RP/0/RP0/CPU0:router(config-un)#commit
```

The following output is an example of configuring a clear-text password that is encrypted using the Type 8 encryption method:

```
RP/0/RP0/CPU0:router(config)# username demo8
RP/0/RP0/CPU0:router(config-un)#secret 0 enc-type 8 PASSWORD
```

The following output is an example of directly configuring a Type 9 encrypted password:

```
RP/0/RP0/CPU0:router(config)#username cisco
RP/0/RP0/CPU0:router(config-un)#secret ?
RP/0/RP0/CPU0:router(config-un)#secret 9
$9$q8j4v/mflSOg5v$nGAhRkf0ek3wSYjDG/VKhwpb2znvPaWusuZtkx9Z1sM
RP/0/RP0/CPU0:router(config-un)#commit
```

The following output is an example of configuring a clear-text password that is encrypted using the Type 9 encryption method:

```
RP/0/RP0/CPU0:router(config)#username cisco
RP/0/RP0/CPU0:router(config-un)#secret 0 enc-type 9 cisco123
RP/0/RP0/CPU0:router(config-un)#commit
```

Configure Secret Type 10

You can use the following options to configure secret Type 10 (that uses SHA512 hashing algorithm) for a user:

Configuration Example:

Directly configuring a Type 10 encrypted password:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#username root secret 10
$6$9UvJidvsTEqgkAPU$3CL1Ei/F.E4v/Hi.UaqLwX8UsSEr9ApG6c5pzhMJmZtgW4jObAQ7meAwyhu5VM/aRFJqe/jxZG17h6xPrvJWf1
RP/0/RP0/CPU0:router(config-un)#commit
```

Configuring a clear-text password that is encrypted using Type 10 encryption method:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#username user10 secret 0 enc-type 10 testpassword
RP/0/RP0/CPU0:router(config-un)#commit
```

CHAPTER 23

Configure Access Control Lists

This procedure describes the access control lists (ACL) and the procedures to configure ACLs.

Table 19: Feature History

Feature Name	Release Information	Feature Description
ACL on Management Port	Cisco IOS XR Release 6.5.31	ACL allows you to control the packets that move through the network. This control allows you to limit the network traffic and restrict the access of users and devices to the network. NCS 4000 supports the following ACL: • ACL1—Ingress ACL on the out-of-band (OOB) management port

Table 20: Feature History

Feature Name	Release Information	Feature Description
ACL on Data Port	Cisco IOS XR Release 6.5.32	ACL allows you to control the packets that move through the network. This control allows you to limit the network traffic and restrict the access of users and devices to the network. ACL is supported on the data port.

Understanding ACL

ACLs perform packet filtering to control the packets that move through the network. These controls allow to limit the network traffic and restrict the access of users and devices to the network. ACLs have many uses, and therefore many commands accept a reference to an access list in their command syntax. An ACL consists of one or more access control entries (ACE) that collectively define the network traffic profile.

Purpose of ACLs

ACLs allow you to perform the following:

- Filter incoming or outgoing packets on an interface.
- Restrict the contents of routing updates.
- Limit debug output that is based on an address or protocol.
- Control vty access.

How an ACL Works

An ACL is a sequential list consisting of permit and deny statements that apply to IP addresses and upper-layer IP protocols. The ACL has a name by which it is referenced. Many software commands accept an ACL as part of their syntax.

An ACL can be configured and named; however, it does not take effect until the ACL is referenced by a command that accepts an ACL. Multiple commands can reference the same ACL. An ACL can control traffic arriving at the router or leaving the router, but not traffic originating at the router.

Source address and destination address are two of the most typical fields in an IP packet on which to base an ACL. Specify source addresses to control packets from certain networking devices or hosts. Specify destination addresses to control packets that are sent to certain networking devices or hosts.

ACLs filter based on standard and extended ACLs to support the filtering of SSH, TACACs, DNS, NTP, ICMP, SNMP, and SYSLOG.

Support of ACLs

NCS 4000 supports the following ACL in R6.5.31:

- ACL1—Ingress IPv4 and IPv6 ACL on the out-of-band (OOB) management port.

NCS 4000 supports the following ACL in R6.5.32:

- Ingress IPv4 ACL on the data port.

Limitations of ACL on Management Port

The following limitations apply to ACL on the management port.

- Only IPv4 and IPv6 with ACL on the management port is supported.
- Ingress IPv4 and IPv6 with ACL on the management port is supported.
- Egress IPv4 and IPv6 with ACL on the management port is not supported.

Configure ACL on Management Port

This procedure describes how to configure the ACL on the IPv4 or IPv6 management port.

Procedure

Step 1 **configure**

Step 2 **interface** *interface-type Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname(config)#
interface MgmtEth0/RP0/EMS/0
```

Enters interface configuration mode.

Step 3 **ipv4 | ipv6 access-group** *access-list-name* **ingress**

Example:

```
RP/0/RP0:hostname(config)#
ipv4 address 209.165.201.1 255.255.255.0
 ipv6 address 2001:db8::1/64
 ipv4 access-group EMS ingress
 ipv6 access-group EMS ingress
!
ipv4 access-list EMS
 10 permit udp any any
!
ipv6 access-list EMS
 10 permit udp any any
!
```

Configures ACL.

Step 4 **commit**

Verify ACL on Management Port

To verify the ACL configuration on the IPv4 or IPv6 management port, use the **show access-lists ipv4** or **show access-lists ipv6** commands.

Note Interface level filter for ACL statistics shows the entire line card statistics instead of specific interface statistics.

```
RP/0/RP0:hostname#show access-lists ipv4
ipv4 access-list CRAFT
10 deny icmp any any
ipv4 access-list EMS
10 deny icmp any any (200 matches)
```

Limitations of ACL on Data Port

The following limitations apply to ACL on the data port.

- Only IPv4 Ingress ACL is supported. IPv4 Egress, IPv6 Ingress, and IPv6 Egress are not supported.
- ACL permit statistics does not increment for the packets that are permitted and getting punted to CPU.
- QoS Ingress policy statistics does not work if ACL is applied on the same interface.
- ACL logging option is not supported.
- ACL fragments option and the ACL on fragmented packets are not supported.
- ACL filtering on BFD, BLB, and BoB packets are not supported.
- ACL statistics are reset to zero upon first read after RP switchover.

The following table describes the support matrix of ACL functional areas and fields.

Table 21: ACL Support Matrix

Area	Protocol or Feature	Direction	Details	Supported
General	IPv4 ACL	ingress	Only ingress IPv4 ACL is supported. No IPv6 support.	Y
Interface Type	IPv4 ACL	ingress	• Layer3 physical interfaces (main or bundle) • Layer3 subinterfaces (main or bundle)	Y

Area	Protocol or Feature	Direction	Details	Supported
Match Fields for IPv4 ACLs	IPv4 ACL			
	Src & Dst IP			Y
	L4 protocol			Y
	IP Prec			Y
	IP DSCP			Y
	L4 src & dst port – exact match			Y
	L4 src & dst port – range			Y
	Match on ICMP			Y
Actions	permit			Y
	deny			Y
Stats (Hit Count)	Both permit & deny			Y

Scale Information for ACL on Data Port

The following table describes the scale information for IPv4 ACL feature in ingress direction.

Table 22: Scale Information for ACL on Data Port

Parameter	Scale Details
Maximum unique ACLs per NPU	31
Maximum ACEs per NPU	300
Maximum permit or deny statistics per NPU	300

Configure ACL on IPv4 Data Port

This procedure describes how to configure the ACL on the IPv4 data port.

Procedure

Step 1 **configure**

Step 2 **interface** *interface-type Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname(config)#
interface FortyGigE0/3/0/7
```

Enters interface configuration mode.

Step 3 **ipv4 address** *ipv4-address subnet-mask*

Example:

```
RP/0/RP0:hostname(config)#ipv4 address 100.1.6.2 255.255.255.252
```

Configures the IPv4 address and subnet mask.

Step 4 **ipv4 access-group** *access-list-name* **ingress**

Example:

```
RP/0/RP0:hostname(config)#ipv4 access-group test_scale_udp_generic ingress
```

Configures ACL.

Step 5 **commit**

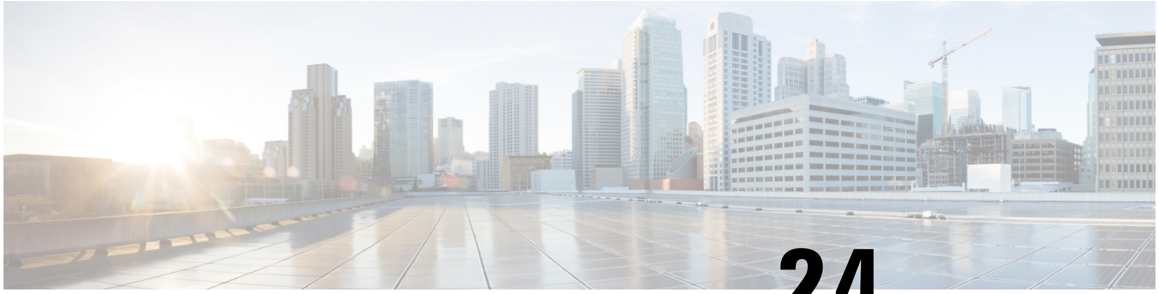
Verify ACL on Data Port

To verify the ACL configuration on the data port, use the **show access-lists** command.

Note Interface level filter for ACL statistics shows the entire line card statistics instead of specific interface statistics.

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

```
RP/0/RP0:hostname#show access-lists test_ro_traffic_generic hardware ingress location 0/lc0
Mon Jun 28 15:29:29.340 IST
ipv4 access-list test_scale_udp_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 (174370 matches)
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
```



CHAPTER 24

Configure LC Priority Shutdown

This chapter describes the procedure to configure the shutdown priority on line cards using IOS.

Configure LC Priority Shutdown

This task enables the LC priority shutdown feature on a NCS 4000 chassis and assigns a shutdown priority on the line cards. For more information, see LC Priority Shutdown, on page 43.

Procedure

Step 1 **configure**

Enters the configuration mode terminal.

Example:

```
RP/0/RP0:hostname# configure
```

Step 2 **power-mgmt progressive location** *rack-id*

Enables the LC priority shutdown feature on the chassis specified and assigns a default priority of 20 to all the line cards.

To disable this feature, use the **no** form of this command.

Example:

```
RP/0/RP0:hostname (config)#power-mgmt progressive location L0
```

Step 3 **priority location** *line-card-location card-priority*

Configures the shutdown priority to the line card specified.

To remove the priority, use the **no** form of this command.

Example:

```
RP/0/RP0:hostname (config-location-L0)#priority location 0/9 6
```

Step 4 **commit**

CHAPTER 25

Configure Controllers

This chapter describes the controllers and procedures to configure the controllers.

Verify a Card State

Before you begin

A card should be inserted on the chassis before verifying a card state.

Procedure

Step 1 **show platform**

Example:

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

Verifies the card details on all the nodes.

Step 2 **show platform**

Example:

```
RP/0/RP0:hostname # admin
```

Enters the admin mode.

Step 3 **show platform**

Example:

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

Verifies the card details on all the nodes.

Example: Verifying a Card State Using XR Prompt

Example: Verifying a Card State Using System Admin Prompt

The following example shows how to verify a card state using Cisco IOS XR commands:

```
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 verify a card state using System Admin Prompt:

```
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
```

Verify the FPGA Firmware Version Using System Admin Prompt

Before you begin

A card should be inserted on the chassis before verifying the firmware version.

Procedure

show hw-module fpd

Example:

```
sysadmin-vm: 0_RP1 # show hw-module fpd
```

Verifies the hardware version on all the cards.

Example: Verifying the Firmware Version Using System Admin Prompt

The following example shows how to verify the firmware version on a card using System Admin Prompt:

```
sysadmin-vm: 0_RP1 # show hw-module fpd
```

```
Wed Apr  15 21:30:22.527 UTC
                                                           FPD Versions
                                                          ===============
Location   Card type      HWver FPD device       ATR Status   Run    Programd
-------------------------------------------------------------------------------
0/1      NCS4K-20T-O-S     0.1   CCC-FPGA          CURRENT   3.23    3.23
0/1      NCS4K-20T-O-S     0.1   CCC-Power-On      CURRENT   1.11    1.11
0/1      NCS4K-20T-O-S     0.1   Ethernet-Switch   CURRENT   1.39    1.39
0/RP0    NCS4K-RP          0.1   Backup BIOS       NEED UPGD         13.06
0/RP0    NCS4K-RP          0.1   Backup-CCC-PwrOn  CURRENT           1.12
0/RP0    NCS4K-RP          0.1   Backup-EthSwitch  CURRENT           1.36
0/RP0    NCS4K-RP          0.1   BP-FPGA           CURRENT   3.16    3.16
0/RP0    NCS4K-RP          0.1   CCC-Bootloader    CURRENT           4.08
0/RP0    NCS4K-RP          0.1   CCC-FPGA          CURRENT   4.08    4.08
0/RP0    NCS4K-RP          0.1   CCC-Power-On      CURRENT   1.12    1.12
0/RP0    NCS4K-RP          0.1   CPU-Complex-Boot  CURRENT           2.04
0/RP0    NCS4K-RP          0.1   CPU-Complex-FPGA  CURRENT   2.04    2.04
0/RP0    NCS4K-RP          0.1   Ethernet-Switch   CURRENT   1.36    1.36
0/RP0    NCS4K-RP          0.1   Primary BIOS      CURRENT   13.08   13.08
0/RP0    NCS4K-RP          0.1   Timing-FPGA       CURRENT   3.13    3.13
```

```
0/RP1    NCS4K-RP          0.1   Backup BIOS       NEED UPGD         13.06
0/RP1    NCS4K-RP          0.1   Backup-CCC-PwrOn  CURRENT           1.12
0/RP1    NCS4K-RP          0.1   Backup-EthSwitch  CURRENT           1.36
0/RP1    NCS4K-RP          0.1   BP-FPGA           CURRENT   3.16    3.16
0/RP1    NCS4K-RP          0.1   CCC-Bootloader    CURRENT           4.08
0/RP1    NCS4K-RP          0.1   CCC-FPGA          CURRENT   4.08    4.08
0/RP1    NCS4K-RP          0.1   CCC-Power-On      CURRENT   1.12    1.12
0/RP1    NCS4K-RP          0.1   CPU-Complex-Boot  CURRENT           2.04
0/RP1    NCS4K-RP          0.1   CPU-Complex-FPGA  CURRENT   2.04    2.04
0/RP1    NCS4K-RP          0.1   Ethernet-Switch   CURRENT   1.36    1.36
0/RP1    NCS4K-RP          0.1   Primary BIOS      CURRENT   13.08   13.08
0/RP1    NCS4K-RP          0.1   Timing-FPGA       CURRENT   3.13    3.13
0/FC0    NCS4016-FC-M      0.1   CCC-FPGA          CURRENT   4.34    4.34
0/FC0    NCS4016-FC-M      0.1   CCC-Power-On      CURRENT   1.11    1.11
0/FC2    NCS4016-FC-M      0.1   CCC-FPGA          CURRENT   4.34    4.34
0/FC2    NCS4016-FC-M      0.1   CCC-Power-On      CURRENT   1.11    1.11
0/FT0    NCS4K-FTA         0.1   Fantray-FPGA      CURRENT   2.08    2.08
0/FT1    NCS4K-FTA         0.1   Fantray-FPGA      CURRENT   2.08    2.08
0/EC0    NCS4K-ECU         0.1   ECU-FPGA          CURRENT   2.08    2.08
```

Verify the FPGA Firmware Version Using XR Prompt

Before you begin

A card should be inserted on the chassis before verifying the firmware version.

Procedure

show hw-module fpd

Example:

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

Verifies the hardware version on all the cards.

Example: Verifying the Firmware Version Using XR Prompt

The following example shows how to verify the firmware version on a card using Cisco IOS XR commands:

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

```
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
```

Verify Craft Firmware Version

Procedure

Step 1 Login into active RP.

Step 2 admin

Example:

```
RP/0/RP0:router# admin
```

Enters SYSADMIN mode.

Step 3 run chvrf 0 bash

Example:

```
sysadmin-vm:0_RP0# run chvrf 0 bash
```

Enters execute mode.

Step 4 /opt/cisco/calvados/sbin/ccc_driver_client

Example:

```
bash-3.2# /opt/cisco/calvados/sbin/ccc_driver_client
```

Displays the CCC Test Client Main Menu.

```
CCC Test client main menu - Version 0.3 - handle with care

  0 ] Refresh menu
  1 ] Watchdog Menu
  2 ] Console Menu
  3 ] CCC Info Menu (Card/Chassis Info/OIR etc)
  4 ] I2C Menu
  5 ] SPI Menu
  6 ] MDIO Menu (PHY's and Marvell)
  7 ] Reset Menu
  8 ] Peek 'n' Poke
  9 ] LED test
  10] EID Menu
  11] Power Control
  12] Craft Panel Tests
  13] Upgrade Bao
  14] PLX eeprom
  15] Sensor Device Menu
  16] Dispaly I2C Logical Config Table
  17] CRE Menu
  18] Atris Config Menu
```

Step 5 Type 12 and press Enter key

Example:

```
12
```

Selects Craft Panel Test option to display the Craft Panel Tests Menu.

```
Craft Panel Tests
        0] Return to the main menu
        1] Transmit a message
        2] Register for receive notifications
        3] Enable/Disable CRAFT UART Loopback
        4] Register for OIR notifications
        5] Get craft panel info
        6] Poke the Craft Panel
        7] Peek the Craft Panel
        8] Read Craft Panel IDPROM
        9] Read Craft Panel Firmware
```

Step 6 Type 9 and press Enter key Select **Read Craft Firmware** from options displayed.

Example:

```
9
```

Dumps the craft firmware number into ccc_driver logs.

```
Server indicated successful craft transmit.
```

Step 7 quit

Exits the execute mode.

Step 8 show controller ccc trace craft_ccc_plugin location "***" | inc CRAFT_FW_VERSION

Example:

```
sysadmin-vm:0_RP0# show controller 1 ccc trace craft_ccc_plugin location "***" | inc
CRAFT_FW_VERSION
```

Note Alternatively execute **show tech ctrace** command and grep for "CRAFT_FW_VERSION" under ccc-driver logs.

```
Tue May  8  08:52:13.685 UTC
2018-05-08:08.51.36.221561844:CR_DLL:_LOG_:craft_decode_rx_msg :[CRAFT_FW_VERSION]<--
"2.9.46tft/hc/L SLCD43 "AT043TN24""
```

Upgrade FPD

Procedure

Step 1 **show hw-module fpd**

Example:

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

or

RP/0/RP0:FPD#show hw-module fpd CCC-FPGA
```

```
or

RP/0/RP0:FPD#show hw-module location 0/FC3 fpd

or

RP/0/RP0:FPD#show hw-module location 0/FC3 fpd CCC-FPGA
```

Displays the current FPD image version. This information determines whether FPD upgrade is required.

Step 2 **show fpd package**

Example:

```
RP/0/RP0:FPD# show fpd package
```

Displays FPD versions compatible with the current software version.

Step 3 **upgrade hw-module location {all |** *slot***} fpd {all |** *fpga-type***} [force]**

Example:

```
RP/0/RP0:FPD# upgrade hw-module location 0/3 fpd all
```

Upgrades the FPD images that need upgrade. If force option is selected then upgrades/downgrades all FPD images.

Note The following FPD's do not have a fallback image:

- Craft FPD

  If the craft FPD upgrade does not complete or fails, the craft might display a blank screen. In such a case rerun the upgrade command.

- PEM FPD

  If the PEM FPD upgrade fails, the module might not work as expected. In such a case rerun the upgrade command.

Step 4 **admin**

Example:

```
RP/0/RP0:FPD# admin
```

Enters into administration exec mode.

Step 5 **hw-module location {** *slot* **} reload**

Example:

```
RP/0/RP0:FPD# hw-module location 0/3 reload
```

(*Optional*) Reloads the card. Required when post upgrade FPD shows RLOAD REQ.

Mapping Type Supported

The following table describes the mapping type supported for NCS4k-24LR-OS line card :

User Provided Info				**Derived Info**	
Port Number	Port Mode	Mapping Type	Framing Type	Payload Type	Data Path
0-23 (1)	ethernet	gmp	opu0	07	24 x 1 GbE over ODU0 over CBRI/GMP mapped on CBRI CBRB ODU0 GMP TTT CPB GE-PMON-Passthrough
10,11, (4) 22,23 (4)	ethernet (LAN)	gfp-f (defined by g.sup43-6.2)	opu2	05	4 x 10GE G.Sup43, 6.2 over ODU2 over CBRI mapped on CBRI CBRB ODU2 GFP-F CPB 10GE-MAC 10GE-PCS
10,11, (4) 22,23 (4)	ethernet (LAN)	bmp (defined by g.sup43-7.1)	opu2e	03	4 x 10GE G.Sup43, 7.1 over ODU2e over CBRI mapped on CBRI CBRB ODU2e BMP CPB 10GERXPMON-Passthrough
10,11, (4) 22,23 (4)	ethernet (LAN)	bmp (defined by g.sup43-7.2)	opu1e	03	4 x 10GE G.Sup43, 7.2 over ODU1e over CBRI mapped on CBRI CBRB ODU2e BMP CPB 10GERXPMON-Passthrough
10,11, (4) 22,23 (4)	ethernet (LAN)	gfp-f-extended (defined by g.sup43-7.3)	opu2	09	4 x 10GE G.Sup43, 7.3 over ODU2 over CBRI (now G.709) mapped on CBRI CBRB ODU2 GFP-F CPB GSUP43-7.3-PCS 10GE_PCS
10,11, (4) 22,23 (4)	ethernet (WAN)	wis (defined by g.sup43-6.1)	opu2	02	4 x 10GE WAN Over Sonet mapped on CBRI CBRB ODU2 GFP-F CPB 10GEMAC WIS(Map/Dem) Sonet-PP STS-192/STM-64
0-3, (2) 6-9, (2) 12-15, (3) 18-21 (3	sonet	bmp	opu1	03	16 x STS-48/STM16 Over ODU1 over CBRI/BMP mapped on CBRI CBRB ODU1 BMP CPB STS-STM-PMON
10,11, (4) 22,23 (4)	sonet	amp	opu2	02	4 x STS-192/STM64 Over ODU2 over CBRI/AMP mapped on CBRI CBRB ODU2 AMP CPB STS-STM-PMON XFI
10,11, (4) 22,23 (4)	sonet	bmp	opu2	03	4 x STS-192/STM64 Over ODU2 over CBRI/BMP mapped on CBRI CBRB ODU2 BMP CPB STS-STM-PMON XFI

User Provided Info				Derived Info	
0-3, (7) 6-9, (7) 12-15, (8) 18-21 (8)	otn	-	opu1	20 or 21 (user provided)	16 x OTU1
10,11, (5) 22,23 (6)	otn	-	opu1e	20 or 21 (user provided)	4 x OTU1e
10,11, (5) 22,23 (6)	otn	-	opu2	20 or 21 (user provided)	4 x OTU2
10,11, (5) 22,23 (6)	otn	-	opu2e	20 or 21 (user provided)	4 x OTU2e
10,11, (5) 22,23 (6)	otn	-	opu1f	20 or 21 (user provided)	4 x OTU1F
10,11, (5) 22,23 (6)	otn	-	opu2f	20 or 21 (user provided)	4 x OTU2F

Following are the limitations for NCS4k-24LR-O-S card:

Note

1. On LR/SFP ports 0..3, GE can be allocated only if 10GE/OC192 traffic is not configured on SFP+ 22; on port 4 GE can be allocated only if OC48 is not configured on port 0; on port 22 GE can be allocated only if OC48 is not configured on port 1. On LR/SFP ports 6..9, GE can be allocated only if 10GE/OC192 traffic is not configured on SFP+ 10; on port 5 GE can be allocated only if OC48 is not configured on port 6; on port 10 GE can be allocated only if OC48 is not configured on port 7.

   On LR/SFP ports 12..15, GE can be allocated only if 10GE/OC192 traffic is not configured on SFP+ 23; on port 16 GE can be allocated only if OC48 is not configured on port 12; on port 23 GE can be allocated only if OC48 is not configured on port 13. On LR/SFP ports 18..21, GE can be allocated only if 10GE/OC192 traffic is not configured on SFP+ 11; on port 17 GE can be allocated only if OC48 is not configured on port 18; on port 11 GE can be allocated only if OC48 is not configured on port 19.

2. OC48 traffic on port 0 can be allocated only if 1GE traffic is not allocated on port 4; OC48 traffic can be allocated on port 1 only if 1GE traffic is not allocated on port 22; OC48 traffic on ports 0..3 can be allocated only if one of 10GE or OC192 is not configured on port 22.

   OC48 traffic on port 6 can be allocated only if 1GE traffic is not allocated on port 5; OC48 traffic can be allocated on port 7 only if 1GE traffic is not allocated on port 10; OC48 traffic on ports 6..9 can be allocated only if one of 10GE or OC192 is not configured on port 10.

3. OC48 traffic on port 12 can be allocated only if 1GE traffic is not allocated on port 16; OC48 traffic can be allocated on port 13 only if 1GE traffic is not allocated on port 23; OC48 traffic on ports 12..15 can be allocated only if one of 10GE or OC192 is not configured on port 23.

   OC48 traffic on port 18 can be allocated only if 1GE traffic is not allocated on port 17; OC48 traffic can be allocated on port 19 only if 1GE traffic is not allocated on port 11; OC48 traffic on ports 18..21 can be allocated only if one of 10GE or OC192 is not configured on port 11.

4. This traffic (10GE/OC192) can be allocated on port 10 only if ports 5..9 do not have any of 1GE or OC48 traffic; 10GE or OC192 can be allocated on port 11 only if ports 17..21 do not have any of 1GE or OC48 traffic; 10GE or OC192 can be allocated on port 22 only if ports 0..4 do not have any of 1GE or OC48 traffic; 10GE or OC192 can be allocated on port 23 only if ports 12..16 do not have any of 1GE or OC48 traffic.
5. This traffic can be configured if the total bandwidth of allocation for OTN traffic on ports 6-9 and 10 is not over 10GBit/Sec, for example, if any OTU2* is allocated on port 10 none of OTU1 can be allocated on ports 6-9; the same is applicable if any of OTU2* is allocated on port 11 none of OTU1 can be allocated on ports 18-21.
6. This traffic can be configured if the total bandwidth of allocation for OTN traffic on ports 0-3 and 22 is not over 10GBit/Sec, for example, if any OTU2* is allocated on port 22 none of OTU1 can be allocated on ports 0-3; the same is applicable if any of OTU2* is allocated on port 23 none of OTU1 can be allocated on ports 12-15.
7. OTU1 traffic can be allocated on ports 0-3 only if ports 22 is not configured with OTU2* traffic; same OTU1 traffic can be allocated on ports 6-9 only if port 10 is not configured with OTU2* traffic.
8. OTU1 traffic can be allocated on ports 12-15 only if ports 23 is not configured with OTU2* traffic; same OTU1 traffic can be allocated on ports 18-21 only if port 11 is not configured with OTU2* traffic.

User Provided Info				**Derived Info**	
Port Number	Port Mode	Mapping Type	Framing Type	Payload Type	Data Path

User Provided Info				Derived Info	
0-19	sonet	amp	opu2	02	OC-192/STM-64 SFP+ over ODU2 mapped to PMON, CPB, AMP Map, Interlaken(CBRI-ODU2)
0-19	sonet	amp	opu2	03	OC-192/STM-64 SFP+ over ODU2 mapped to PMON, CPB, BMP Map, Interlaken(CBRI-ODU2)
0-19	ethernet (LAN)	gfp-f (defined by g.sup43-6.2)	opu2	05	10GE SFP+ over ODU2 mapped to Rx MAC+PCS, CPB, GFP-F Map (G.Sup43 6.2)
0-19	ethernet (LAN)	gfp-f (defined by g.sup43-7.1)	opu2e	03	10GE SFP+ over ODU2e mapped to PMON, 10GE Rx Passthru, CPB, BMP Map (G.Sup43 7.1), Interlaken(CBRI - ODU2e)
0-19	ethernet (LAN)	gfp-f (defined by g.sup43-7.3)	opu2	09	10GE SFP+ over ODU2 mapped to PMON, 10GE Rx Passthru, CPB, GFP-F Map (G.Sup43 7.3), Interlaken(CBRI - ODU2)
0-19	ethernet (WAN)	gfp-f	opuflex	09	10GE SFP+ over ODUFlex mapped to Rx MAC+PCS, CPB, GFP-F Map Interlaken(CBRI - ODUflex)
0-19	otn	-	opu1e	20 or 21 (user provided)	OTU1e
0-19	otn	-	opu2	20 or 21 (user provided)	OTU2
0-19	otn	-	opu2e	20 or 21 (user provided)	OTU2e
0-19	otn	-	opu1f	20 or 21 (user provided)	OTU1F
0-19	otn	-	opu2f	20 or 21 (user provided)	OTU2F

User Provided Info				Derived Info	
Port Number	Port Mode	Mapping Type	Framing Type	Payload Type	Data Path
0,1	ethernet	gfp-f	opu4	05	100GE NCS4K-2H-O-K over ODU4 mapped to Rx MAC+PCS, CPB, GFP-F Map (G.Sup43 6.2)
0,1	ethernet	amp	opu4	09	100GE NCS4K-2H-O-K over ODU4 mapped to PMON, 100GE Rx Passthru, CPB, GMP Map, Interlaken(CBRI – ODU4)
0,1	ethernet	gfp-f	opuflex	05	100GE NCS4K-2H-O-K over ODUFlex mapped to Rx MAC+PCS, CPB, GFP-F Map Interlaken(CBRI - ODUflex)
0,1	otn	-	opu4	21	OTU4

Configure an OTN Controller

Before you begin

Optics controller should be created before configuring an OTN controller and must be in UP state.

Procedure

Step 1 **configure**

Step 2 controller **optics** *Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname# controller optics 0/0/0/0
```

Enters the Optics controller mode.

Step 3 **port-mode {Ethernet | FC | OTN | SDH | Sonet} framing** *framing-type* **mapping** *mapping-type*

Example:

```
RP/0/RP0:hostname(config-optics)# port-mode sdh framing opu1 mapping amp
```

Configures the port-mode for the sdh controller. Mapping is not required for otn controllers.

Step 4 **commit**

Example: Configure Port Mode as OTN

The following example shows how to configure port mode as otn using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname# controller optics 0/0/0/0
```

```
RP/0/RP0:hostname(config-optics)# port-mode otn framing opu2
RP/0/RP0:hostname(config-optics)# exit
```

Configure the LAN PHY Controller

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the configuration mode.

Step 2 **controller optics** *R/S/I/P*

Example:

```
RP/0/RP0:hostname(config)# controller optics 0/6/0/1
```

Enters the optics controller configuration mode.

Step 3 **port-mode Ethernet framing packet rate** *rate*

Example:

```
RP/0/RP0:hostname (config-Optics)# port-mode Ethernet framing packet rate 100GE
```

Configures the port-mode for the Ethernet controller.

Step 4 **commit**

Example:

```
RP/0/RP0:hostname(config-Optics)# commit
```

Example: Configure LAN PHY controller interface:

The following example shows how to configure a 100GE LAN PHY controller interface HundredGigE0/6/0/1 using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# controller optics 0/6/0/1
RP/0/RP0:hostname(config-Optics)# port-mode Ethernet framing packet rate 100GE
RP/0/RP0:hostname(config-Optics)# commit
```

The following example shows how to configure a 10GE LAN PHY controller interface TenGigE0/14/0/2 using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# controller optics 0/14/0/2
RP/0/RP0:hostname(config-Optics)# port-mode Ethernet framing packet rate 10GE
RP/0/RP0:hostname(config-Optics)# commit
```

Configure the Ethernet terminated OTN Controller (without Breakout)

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the configuration mode.

Step 2 **controller optics** *R/S/I/P*

Example:

```
RP/0/RP0:hostname(config)# controller optics 0/6/0/1
```

Enters the optics controller configuration mode.

Step 3 **port-mode OTN framing** *framing type*

Example:

```
RP/0/RP0:hostname (config-Optics)# port-mode OTN framing opu4
```

Configures the port-mode for the OTN controller.

Step 4 **exit**

Example:

```
RP/0/RP0:hostname (config-Optics)# exit
```

Exits the sub mode.

Step 5 **controller** *payload-type R/S/I/P*

Example:

```
RP/0/RP0:hostname(config)# controller ODU4 0/6/0/1
```

Enters the odu controller configuration mode.

Step 6 **terminate ether mapping** *mapping-type*

Example:

```
RP/0/RP0:hostname(config - odu4)# terminate ether mapping GfpF
```

Step 7 **commit**

Example:

```
RP/0/RP0:hostname(config-odu4)# commit
```

Example: Configure LAN PHY controller interface:

The following example shows how to configure a 100GE Ethernet terminated OTN controller interface HundredGigE0/6/0/1 using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# controller optics 0/6/0/1
RP/0/RP0:hostname(config-Optics)# port-mode OTN framing opu4
RP/0/RP0:hostname(config-Optics)# exit
RP/0/RP0:hostname(config)# controller ODU4 0/6/0/1
RP/0/RP0:hostname(config-odu4)# terminate ether mapping GfpF
RP/0/RP0:hostname(config-odu4)# commit
```

The following example shows how to configure a 10GE Ethernet terminated OTN controller interface TenGigE0/14/0/2 using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# controller optics 0/14/0/2
RP/0/RP0:hostname(config-Optics)# port-mode OTN framing opu2e
RP/0/RP0:hostname(config-Optics)# exit
RP/0/RP0:hostname(config)# controller ODU2E 0/14/0/2
RP/0/RP0:hostname(config-odu2e)# terminate ether mapping bmp
RP/0/RP0:hostname(config-odu2e)# commit
```

Configure the Ethernet terminated OTN Controller (with Breakout)

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the configuration mode.

Step 2 **controller optics** *R/S/I/P* **breakout-mode** *lane id* **otn framing** *framing type*

Note All lanes should be configured in same mode.

Only opu2 and opu2e framing type are supported.

Example:

```
RP/0/RP0:hostname(config)# controller optics 0/0/0/1 breakout-mode 3 otn framing opu2
```

Step 3 **exit**

Example:

```
RP/0/RP0:hostname (config-Optics)# exit
```

Exits the sub mode.

Step 4 **controller { ODU2 | ODU2E }** *R/S/I/P/lane-id* **terminate ether mapping** *{ GfpF | bmp }*

Example:

```
RP/0/RP0:hostname(config)# controller ODU2 0/0/0/1/3 terminate ether mapping GfpF
```

Step 5 **commit**

Example:

```
RP/0/RP0:hostname(config-odu2)# commit
```

Example

The following examples show how to configure a TenGigE0/0/0/1/3 interface using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# controller optics 0/0/0/1 breakout-mode 3 otn framing opu2
RP/0/RP0:hostname(config-Optics)# exit
RP/0/RP0:hostname(config)# controller ODU2 0/0/0/1/3 terminate ether mapping GfpF
RP/0/RP0:hostname(config-odu2)# commit
```

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# controller optics 0/0/0/1 breakout-mode 3 otn framing opu2e
RP/0/RP0:hostname(config-Optics)# exit
RP/0/RP0:hostname(config)# controller ODU2e 0/0/0/1/3 terminate ether mapping bmp
RP/0/RP0:hostname(config-odu2)# commit
```

The following examples show how to configure a fourty gigabit interface using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# controller Optics0/4/0/5
breakout-mode 1 Otn framing opu2
breakout-mode 2 Otn framing opu2
breakout-mode 3 Otn framing opu2
breakout-mode 4 Otn framing opu2
!
RP/0/RP0:hostname(config-Optics)# exit
RP/0/RP0:hostname(config)# controller ODU20/4/0/5/1
 terminate ether mapping GfpF
!
controller ODU20/4/0/5/2
 terminate ether mapping GfpF
!
controller ODU20/4/0/5/3
 terminate ether mapping GfpF
!
controller ODU20/4/0/5/4
 terminate ether mapping GfpF
!

RP/0/RP0:hostname(config-odu2)# commit
```

Configure the Clock Controller

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the configuration mode.

Step 2 **clock-interface** [**Rack0-Bits0-In** | **Rack0-Bits0-Out** | **Rack0-Bits1-In** | **Rack0-Bits1-Out**]

Example:

```
RP/0/RP0:hostname(config)# clock-interface Rack0-Bits0-Out
```

Enters the clock interface configuration mode.

Step 3 **port-parameters** [**Interface Type**] [**bits-input** | **bits-output**] **[BITS mode]**

Note Refer following table for configuring port parameters:

BITS mode	Interface Type	QL Option	Supported as Input	SSM Rx Supported	Supported as Output	SSM Tx Supported
T1 D4 AMI	ANSI (Wirewrap)	O2 G1	Yes	No - use receive exact	Yes	No - ssm disabled
T1 D4 B8ZS	ANSI (Wirewrap)	O2 G1	Yes	No - use receive exact	Yes	No - ssm disabled
T1 ESF AMI	ANSI (Wirewrap)	O2 G1	Yes	Yes	Yes	Yes
T1 ESF B8ZS	ANSI (Wirewrap)	O2 G1	Yes	Yes	Yes	Yes
J1 D4 AMI	ANSI (Wirewrap)	O2 G1	Yes	No - use receive exact	Yes	No - ssm disabled
J1 D4 B8ZS	ANSI (Wirewrap)	O2 G1	Yes	No - use receive exact	Yes	No - ssm disabled
J1 ESF AMI	ANSI (Wirewrap)	O2 G1	Yes	Yes	Yes	Yes
J1 ESF B8ZS	ANSI (Wirewrap)	O2 G1	Yes	Yes	Yes	Yes
E1 FAS AMI	ETSI (BNC)	O1	Yes	Yes	Yes	Yes

E1 FAS HDB3	ETSI (BNC)	O1	Yes	Yes	Yes	Yes
E1 CRC4 AMI	ETSI (BNC)	O1	Yes	Yes	Yes	Yes
E1 CRC4 HDB3	ETSI (BNC)	O1	Yes	Yes	Yes	Yes
E1 G.703 2048KHz	ETSI	O1	Yes	No - use receive exact	Yes	No - ssm disabled
64KHz + 8KHz Composite Clock (Includes GR378 and G.703)	ANSI & ETSI	O1/O2	Yes	No - use receive exact	No	No

Example:

```
RP/0/RP0:hostname (config-clock-if)# port-parameters etsi bits-output e1 crc-4 sa4 ami
```

Configures the port-parameters for the clock controller.

Step 4 **commit**

Example:

```
RP/0/RP0:hostname(config-clock-if)# commit
```

Example: Configure Clock controller interface:

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
```

Configure 100MHZ Flex Grid for NCS4K-4H-OPW-QC2 Line Card

Table 23: Feature History

Feature Name	Release Information	Feature Description
100MHz Grid Spacing for NCS4K-4H-OPW-QC2 line card	Cisco IOS XR Release 6.5.33	In addition to the 50GHZ flex-grid-spacing, you can now configure 100MHz flex-grid-spacing on the CFP2 trunk ports of the NCS4K-4H-OPW-QC2 card. The setup can be done by Cisco Transport Controller (CTC) or CLI. With 100MHz flex-grid-spacing, you can configure up to 761 different wavelengths; which is more than 96 wavelengths that can be done with 50GHZ flex-grid-spacing. Commands added: • dwdm-carrier Commands modified: • show controller optics

The trunk ports 10 and 11 with coherent CFP2 optics in the NCS4K-4H-OPW-QC2 card currently support 50GHz grid spacing. However, the coherent CFP2 optics supports 100MHz grid spacing. From Release 6.5.33, you can configure 100MHz flex grid spacing. The 100MHz grid spacing enables you to configure the frequencies with a granularity of 7 digits, and therefore 761 different wavelengths can be configured on the colored optics, whereas 50GHz grid spacing can support only 96 wavelengths.

You can also configure the 100MHz grid spacing through CTC. See Configure 100MHz Grid Spacing for NCS4K-4H-OPW-QC2 Line Card Using CTC, on page 52.

Procedure

Step 1 **configure**

```
RP/0/RP0:hostname# configure
```

Enters the configuration mode.

Step 2 **controller optics** *Rack/Slot/Instance/Port*

```
RP/0/RP0:hostname(config)#controller optics 0/0/0/11
```

Enters the optics controller configuration mode.

Step 3 **shutdown**

```
RP/0/RP0:ios(config-Optics)#shutdown
```

Shuts down the controller.

Step 4 **sec-admin-state maintenance**

```
RP/0/RP0:ios(config-Optics)#sec-admin-state maintenance
```

Configures the administrative state of the controller to maintenance mode.

Step 5 **dwdm-carrier 100MHz-grid frequency** *<frequency-value>*

The frequency range is 1911500-1961000. In 100MHz grid spacing, enter the 7-digit frequency value in the range of 1911500 to 1961000 THz. For example, enter 1913501 to specify 191.3501 THz.

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

Configures the wavelength in 100MHz (0.1GHz) grid spacing in accordance with ITU definition.

Step 6 **commit**

Step 7 **no shutdown**

```
RP/0/RP0:ios(config-Optics)# no shutdown
```

Brings up the controller.

Step 8 **commit**

Step 9 **show controller optics** ***R/S/I/P*** **dwdm-carrier-map flexi-grid**

```
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--
```

Displays the wavelength and channel mapping with flexible grid channel spacing enabled.

Configure an OTU (HO/LO) Controller

Before you begin

Optics controller should be created before configuring an OTU (HO/LO) controller and must be in UP state.

Procedure

Step 1 **configure**

Step 2 **controller otu** [HO | LO] *R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller OTU1 0/0/0/1
```

Enters the otu controller configuration mode.

Step 3 **fec** *{EnhancedHG20 | EnhancedHG7 | EnhancedI4 | EnhancedI7 | EnhancedSwizzle | Standard | None}*

Example:

```
RP/0/RP0:hostname (config-otu1)# fec EnhancedHG20
```

Configures FEC on the otu controller.

Step 4 **gcc0**

Example:

```
RP/0/RP0:hostname (config-otu1)# gcc0
```

Configures GCC on the otu controller.

Step 5 **secondary-admin-state** *[Automatic-in-service | Maintenance | Normal]*

Example:

```
RP/0/RP0:hostname (config-otu1)# secondary-admin-state maintenance
```

Configures the secondary administrative state of an otu controller.

Step 6 **loopback** *[internal | line]*

Example:

```
RP/0/RP0:hostname (config-otu1)# loopback internal
```

Configures loopback mode of an otu controller.

Step 7 **threshold {sd | sf | sm-tca}** *value*

Example:

```
RP/0/RP0:hostname (config-otu1)# threshold sf 7
```

Configures the threshold for signal failure and signal degrade on the OTUk controller.

The valid range of signal failure is from 1 to 9 and for signal degrade is from 3 to 9.

The valid range of sm-tca is from 3 to 9. The default range is 3.

Step 8 **tti [expected | sent]** *{ascii | dapi | hex | operator-specific | sapi} value*

Example:

```
RP/0/RP0:hostname (config-otu1)#  tti expected ascii abc
```

Configures the trail trace identifier (TTI) of an otu controller. The maximum length of the ascii text is 64 characters.

Step 9 **srlg set** *index-of-the-srlg value-of-the-network-srlg*

Example:

```
RP/0/RP0:hostname (config-otu1)#  srlg set 5 8 6 7 8 9 7
```

Configures the SRLG for network. The valid range of index is from 1 to 17.

The valid range of values is from 0 to 4294967294. You can set a maximum of six values in one set.

Step 10 **commit**

Example: Configure an otu Controller

The following example shows how to configure an otu controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# controller otu1 0/0/0/1
RP/0/RP0:hostname(config-otu1)# fec EnhancedHG20
RP/0/RP0:hostname(config-otu1)# gcc0
RP/0/RP0:hostname(config-otu1)# secondary-admin-state maintenance
RP/0/RP0:hostname(config-otu1)# loopback internal
RP/0/RP0:hostname(config-otu1)#threshold sf 7
RP/0/RP0:hostname(config-otu1)#tti expected ascii abc
RP/0/RP0:hostname(config-otu1)#srlg set 5 8 6 7 8 9 7
RP/0/RP0:hostname(config-otu1)#exit
```

Configure an ODU (HO/LO) Controller

Before you begin

Optics controller should be created before configuring an ODU (HO/LO) controller and must be in UP state.

Procedure

Step 1 **configure**

Step 2 **controller odu**_[HO | LO] R/S/I/P_

Example:

```
RP/0/RP0:hostname (config)# controller ODU1 0/0/0/1
```

Enters the ODU controller configuration mode.

Step 3 **gcc1**

Example:

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

Configures GCC on the ODU controller. To remove gcc use no form of this command.

Step 4 **secondary-admin-state** _[Automatic-in-service | Maintenance | Normal]_

Example:

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

Configures the secondary administrative state of the ODU controller. Administrative state can be normal and maintenance.

Step 5 **loopback** _[internal | line]_

Example:

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

Configures loopback mode of the ODU controller. You can configure the line and internal loopback modes.

Step 6 **threshold {pm-tca | sf | sd}** _value_

Example:

```
RP/0/RP0:hostname (config-odu1)# threshold sf 7
RP/0/RP0:hostname (config-odu1)# threshold sd 5
RP/0/RP0:hostname (config-odu1)# threshold pm-tca 6
```

Configures the threshold for signal failure, signal degrade and pm-tca on the ODU controller.

Sets the signal fail bit error rate. The range is for NCS4K-20T-O-S and NCS4K-20T-O-S is from 1E-6 to 1E-9. The default value is 6. The range for other cards is from 1E-5 to 1E-9. The default value is 5.

Sets the signal degrade bit error rate. The range is from 1E-3 to 1E-9. The range is for NCS4K-20T-O-S and NCS4K-20T-O-S is from 1E-6 to 1E-9. The default value is 7. The range for other cards is from 1E-5 to 1E-9. The default value is 7

The valid range of pm-tca is from 3 to 9. The default value is 6.

Step 7 **tsg** _[1.25G | 2.5G]_

Example:

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

Configures TSG of the ODU controller. The valid values are 1.25G and 2.5G.

Step 8 **tti [expected | sent]** _{ascii | dapi | hex | operator-specific | sapi} value_

Example:

```
RP/0/RP0:hostname (config-odu1)# tti expected ascii abc
```

Configures the TTI of the ODU controller. The maximum length of the ascii text is 64 characters.

Step 9 **tcm id** *value*

Example:

```
RP/0/RP0:hostname (config-odu1)# tcm id 4
```

Configures the TCM level for the ODU controller and enters the TCM mode. The valid range is from 1 to 6.

Step 10 **threshold {pm-tca | sf | sd}** *value*

Example:

```
RP/0/RP0:hostname (config-odu1-tcm0x4)# threshold sd 5

RP/0/RP0:hostname (config-odu1-tcm0x4)# threshold sf 7

RP/0/RP0:hostname (config-odu1-tcm0x4)# threshold pm-tca 7
```

Configures the threshold for signal failure and signal degrade in the TCM connection.

The valid range of signal failure is from 1 to 9. The default value is 3.

The valid range of signal degrade is from 3 to 9. The default value is 6.

The valid range of pm-tca is from 3 to 9. The default value is 3.

Step 11 **tti [expected | sent] {ascii | dapi | hex | operator-specific | sapi}** *value*

Example:

```
RP/0/RP0:hostname (config-odu1-tcm0x4)# tti expected ascii abc
```

Configures the TTI of the TCM controller. The maximum length of the ascii text is 64 characters.

Step 12 **commit**

Example: Configure an ODUk Controller

The following example shows how to configure an ODU controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)#controller ODU1 0/0/0/1
RP/0/RP0:hostname(config-odu1)#gcc1
RP/0/RP0:hostname(config-odu1)#secondary-admin-state maintenance
RP/0/RP0:hostname(config-odu1)#loopback internal
RP/0/RP0:hostname(config-odu1)#threshold sf 7
RP/0/RP0:hostname(config-odu1)#tsg 1.25G
RP/0/RP0:hostname(config-odu1)#tti expected ascii abc
RP/0/RP0:hostname(config-odu1)#tcm id 4
RP/0/RP0:hostname(config-odu1-tcm0x4)#threshold sd 5
RP/0/RP0:hostname(config-odu1-tcm0x4)#tti expected ascii abc
RP/0/RP0:hostname(config-odu1-tcm0x4)#exit
```

Configure Squelch for ODU Controller

Procedure

Step 1 **configure**

Enters the global configuration mode.

Step 2 **controller ODU2** *R/S/I/P*

Example:

```
RP/0/RP0:hostname(config)#controller ODU2 0/1/0/1
```

Enters the ODU2 controller mode.

Step 3 **opu ca laser-squelch** *hold-off timer*

Example:

```
RP/0/RP0:hostname(config-odu2)#opu ca laser-squelch 20
```

Configures squelch hold-off time. The range is 20ms to 10000 ms.

Step 4 **commit**

Configure Idle Frame for ODU Controller

Procedure

Step 1 **configure**

Enters the global configuration mode.

Step 2 **controller ODU2** *R/S/I/P*

Example:

```
RP/0/RP0:hostname(config)#controller ODU2 0/1/0/1
```

Enters the ODU2 controller mode.

Step 3 **opu ca idle-frame** *hold-off timer*

Example:

```
RP/0/RP0:hostname(config-odu2)#opu ca laser-squelch 20
```

Configures idle frame hold-off time. The range is 20ms to 10000 ms.

Step 4 **commit**

Configure an ODU Group Controller

Before you begin

Optics controller should be created before configuring an ODU controller and must be in UP state.

Procedure

Step 1 **configure**

Step 2 **controller [odu-group-mp | odu-group-te]***group-id* **signal {Ethernet | FC | OTN | SDH | Sonet} odu-type** *type-of-the-odu*

Example:

```
RP/0/RP0:hostname# controller odu-group-mp 5 signal OTN odu-type odu1
```

This creates the ODU group controller. The ODU Group MP value ranges from 1 to 65535.

Step 3 **commit**

Configure the Ethernet Controller

Before you begin

Optics controller should be created before configuring an Ethernet controller and must be in UP state.

Procedure

Step 1 **configure terminal**

Example:

Router# configure terminal

Enters the global configuration mode.

Step 2 controller **optics** *R/S/I/P* **port-mode ethernet framing** *type* **mapping** *type* **rate** *rate*

Note The **rate** parameter will appear only if the framing type is opuflex.

Example:

```
RP/0/RP0:hostname# controller optics 0/0/0/0 port-mode ethernet framing opuflex mapping
GfpF rate 100GE
```

Configures the port-mode for the ethernet controller.

Step 3 **exit**

Example:

Router(config-oc3)# exit

Exits the OC controller configuration mode.

Example: Configure Port Mode as Ethernet

The following example shows how to configure port mode as ethernet using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# controller optics 0/0/0/0 port-mode Ethernet framing opuflex
mapping GfpF rate 100GE
RP/0/RP0:hostname(config)# commit
```

Configure a SONET or SDH Controller

Before you begin

Optics controller should be created before configuring a SONET or SDH controller and must be in UP state.

Procedure

Step 1 **configure**

Step 2 controller **optics** *Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname# controller optics 0/0/0/2
```

Enters the optics controller mode.

Step 3 **port-mode {Ethernet | FC | OTN | SDH | SONET} framing** *framing-type* **mapping** *mapping-type* **rate** *{ OC3 | OC12 | STM1 | STM4 }*

Example:

```
RP/0/RP0:hostname(config-optics)# port-mode sonet framing opu1 mapping bmp
```

Configures the port-mode for the SONET or SDH controller. New parameter rate is introduced for oc3, oc12, stm1 and stm4 controllers.

Note You can create SONET controller when the mapping type is amp and framing type is opu1 only (optics->sonet -> sonet sdh -> odu1).

Step 4 **commit**

Example: Configure Port Mode as SONET

The following example shows how to configure port mode as SONET using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname# controller optics 0/0/0/2
RP/0/RP0:hostname(config-optics)# port-mode SONET framing opu1 mapping bmp
RP/0/RP0:hostname(config-optics)# exit
```

Configure an OCn controller

Before you begin

Optics controller should be created before configuring an OCn controller and must be in UP state.

Procedure

Step 1 **configure**

Step 2 controller **oc***n Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname# controller oc48 0/0/0/2
```

Enters the oc48 controller mode.

Step 3 **clock source [internal | line]**

Example:

```
RP/0/RP0:hostname (config-oc48)# clock source internal
```

Configures the clock source on an OCn controller.

Step 4 **threshold {b1-tca | b2-tca | sd-ber | sf-ber}** *value*

Example:

```
RP/0/RP0:hostname (config-oc48)# threshold b1-tca 6
```

Configures the bit error rate (BER) on threshold crossing alert (TCA) of a controller. 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.

Step 5 **overhead j0 [expected | send] [16Bytes | 1Byte]** *value*

Example:

```
RP/0/RP0:hostname (config-oc48)# overhead j0 extected 1Byte 45
```

Configures a 1 Byte path trace on OCn controller. The byte value ranges from 0 to 255.

Step 6 **commit**

Example: Configure OCn controller

The following example shows how to configure OCn controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
```

```
RP/0/RP0:hostname(config)# controller oc48 0/0/0/2
RP/0/RP0:hostname(config-oc48)# clock source internal
RP/0/RP0:hostname(config-oc48)# threshold b1-tca 6
RP/0/RP0:hostname(config-oc48)# overhead j0 expected 1Byte 45
RP/0/RP0:hostname(config-oc48)# exit
```

Configure a STSn Controller

Before you begin

Optics controller should be created before configuring a STSn controller and must be in UP state.

Note STSn path can be configured on WIS port only

Procedure

Step 1 **configure**

Step 2 **controller sts***n R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller sts48 0/0/0/2
```

Enters the STS48 controller configuration mode.

Step 3 **threshold b3-tca** *value*

Example:

```
RP/0/RP0:hostname (config-sts48)# threshold b3-tca 7
```

Configures the bit error rate (BER) on threshold crossing alert (TCA) of the controller. The BER value ranges from 3 to 9 and default value is 6.

Step 4 **overhead j1 [expected | send] [16Bytes | 64Bytes]** *ASCII text*

Example:

```
RP/0/RP0:hostname (config-sts48)# overhead j1 expected 64Bytes abcx
```

Configures the 64Bytes path trace on the STSn controller.

Step 5 **commit**

Example: Configure an STSn Controller

The following example shows how to configure an STSn controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# controller sts48n 0/0/0/2
RP/0/RP0:hostname(config-sts48)# threshold b3-tca 7
RP/0/RP0:hostname(config-sts48)# overhead j1 expected 64Bytes abcx
```

```
RP/0/RP0:hostname(config-sts48)# exit
```

Configure a STMn controller

Before you begin

Optics controller should be created before configuring a STMn controller and must be in UP state.

Procedure

Step 1 **configure**

Step 2 **controller stm***n R/S/I/P*

Example:

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

Enters the STM64 controller configuration mode.

Step 3 **clock source [internal | line]**

Example:

```
RP/0/RP0:hostname (config-stm64)# clock source internal
```

Configures the clock source on an stm controller.

Step 4 **threshold {b1-tca | b2-tca | sd-ber | sf-ber}** *value*

Example:

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

Configures the bit error rate (BER) on threshold crossing alert (TCA) of a controller. 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.

Step 5 **overhead j0 [expected | send] [16Bytes | 1Byte]** *Ascii value*

Example:

```
RP/0/RP0:hostname (config-stm64)# overhead j0 expected 16Bytes abcx
```

Configures a 16 Bytes path trace on the stm controller.

Step 6 **commit**

Example: Configure STM controller

The following example shows how to configure STM controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# controller stm64 0/0/0/2
RP/0/RP0:hostname(config-stm64)# clock source internal
```

```
RP/0/RP0:hostname(config-stm64)# threshold b2-tca 7
RP/0/RP0:hostname(config-stm64)# overhead j0 expected 16Bytes abcx
RP/0/RP0:hostname(config-stm64)# exit
```

Configure a VCn Controller

Optics controller should be created before configuring a VCn controller and must be in UP state.

Note VCk path can be configured on WIS port.

Procedure

Step 1 **configure**

Step 2 **controller vc***n R/S/I/P*

Example:

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

Enters the vc4-64c configuration mode.

Step 3 **threshold b3-tca** *value*

Example:

```
RP/0/RP0:hostname (config-vc4-64c)# threshold b3-tca 8
```

Configures the bit error rate (BER) on threshold crossing alert (TCA) of the controller.

Step 4 **overhead j1 [expected | send] [16Bytes | 64Bytes]** *Ascii value*

Example:

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

Configures a 64Bytes path trace on the VCk controller.

Step 5 **commit**

Example: Configure a VCk Controller

The following example shows how to configure a VCn controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# controller vc4-64c 0/0/0/10
RP/0/RP0:hostname(config-vc4-64c)# threshold b3-tca 8
RP/0/RP0:hostname(config-vc4-64c)# overhead j1 send 64Bytes abcz
RP/0/RP0:hostname(config-vc4-64c)# exit
```

Channelize an ODU (LO) Controller

Before you begin

Optics controller should be created before configuring an ODU (LO) controller.

Procedure

Step 1 **configure**

Step 2 **controller odu** *j R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller odu4 0/0/0/2
```

Enters the ODUj controller configuration mode.

Step 3 **odu** *j* **tpn** *number-of-the-tributary-port* **ts** *slot-of-the-tributary*

Example:

```
RP/0/RP0:hostname (config)# (config-odu4)# ODU3 tpn 4 ts 1-2
```

Creates a lower order ODU controller and configures tributary port number (TPN) and tributary slots (TS) for that ODU controller. The valid range of TPN is from 1 to 80.

The TS string can be separated from 1 to the number of TS in the parent controller by a colon (:) or an en-dash (-). If a TS string is separated using a colon (:), this indicates individual tributary slot. If a TS string is separated using an en-dash (-), this indicates a range of tributary slots.

Note To configure the packet interface, you need to terminate the configurations using command: **terminate ether mapping GfpF/bmp**

Step 4 **commit**

Configure AINS

This task configures AINS for the controller. For more information on AINS support, see AINS Support for Controllers, on page 45.

Procedure

Step 1 **automatic-in-service controller** ***controller-name R/S/I/P*** **hours** ***x*** **minutes** ***y***

Configures AINS with a soak timer of 15 minutes.

Note To clear the AINS configuration set the hours and minutes to 0.

Example:

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

Step 2 **show controller** ***controller -name R/S/I/P***

Displays the AINS parameters that have been configured.

Example:

```
RP/0/RP0:hostname# sh controllers optics 0/6/0/2
Tue Aug 14 03:52:22.279 UTC
 Controller State: Up
 Transport Admin State: Automatic In Service
 Laser State: On
  Optics Status
         Optics Type:  Grey optics
         Wavelength = 850.00 nm
         Alarm Status:
         -------------
         Detected Alarms: None
         LOS/LOL/Fault Status:
         Alarm Statistics:
         -------------
         HIGH-RX-PWR = 0            LOW-RX-PWR = 0
         HIGH-TX-PWR = 0            LOW-TX-PWR = 1
         HIGH-LBC = 0               HIGH-DGD = 0
         OOR-CD = 0                 OSNR = 0
         WVL-OOL = 0                MEA  = 0
         IMPROPER-REM = 0
         TX-POWER-PROV-MISMATCH = 0
         Laser Bias Current = 52.0 %
         Actual TX Power = -2.41 dBm
         RX Power = -3.55 dBm
         Performance Monitoring: Enable
         THRESHOLD VALUES
         ----------------
         Parameter                 High Alarm  Low Alarm  High Warning  Low Warning
         ------------------------  ----------  ---------  ------------  -----------
         Rx Power Threshold(dBm)          1.5      -12.4           0.0          0.0
         Tx Power Threshold(dBm)          1.2       -9.8           0.0          0.0
         LBC Threshold(mA)                N/A        N/A          0.00         0.00
         LBC High Threshold = 98 %
         Polarization parameters not supported by optics
 Transceiver Vendor Details
         Form Factor            : SFP+
 AINS Soak                : Running
 AINS Timer               : 0h, 15m
 AINS remaining time      : 896 seconds
```

Clear the Traffic from a Resource in an ODU Group Controller

Perform this task to clear the traffic from a resource in an odu group controller.

Procedure

Step 1 **configure**

Step 2 **odu-group {mp | te} group id-of-the-odu-group-mp | te clear odu-dest** *name-of-the-controller Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname Router# controller odu-group-mp 1 manual odu-dest odu0 0/0/0/1
```

Clears the traffic from the ODU0 controller in a network

Step 3 **commit**

Aggregation of Traffic in OTN

An OTN circuit carries multiple data streams from various sources. It also carries non-OTN data streams (SONET) coming at any rate. These multiple data streams from various sources are combined and transmitted over a single data stream and this is done through multiplexers.

During multiplexing, various weak data streams are converted into a single strong data stream and then a de-multiplexer is used to transmit the data in their respective formats to the destination. This entire process is called OTN aggregation.

Remove and Install Fabric Card Using System Admin Prompt

Before you begin

A card should be inserted on the chassis before you remove it or plug it to another chassis.

Procedure

Step 1 **controllers fabric plane *plane-id* shutdown**

Example:

```
sysadmin-vm: 0_RP0 # conf t
```

Enters the configuration mode terminal.

Example:

```
sysadmin-vm: 0_RP0 # controller fabric plane 3 shutdown
```

Example:

```
sysadmin-vm: 0_RP0 # commit
```

Step 2 Remove the card physically.

Step 3 Insert the card manually.

Example:

```
sysadmin-vm: 0_RP0(config) # show controller sfe driver rack 0
```

When the output of this command displays DONE and NRML entry for all the fabric cards, perform the next step. Else, there might be traffic loss.

Example:

```
+--------------------------------------------------------------------------+
| Asic inst.|card|HP|Asic| Admin|plane| Fgid| Asic State |DC| Last  |PON|HR |
|  (R/S/A)  |pwrd|  |type| /Oper|/grp | DL  |            |  | init  |(#)|(#)|
+--------------------------------------------------------------------------+
| 0/FC3/0   | UP | 1|s123| UP/UP| 3/A | DONE| NRML       | 0| PON   |  1|  0|
| 0/FC3/1   | UP | 1|s123| UP/UP| 3/A | DONE| NRML       | 0| PON   |  1|  0|
| 0/FC3/2   | UP | 1|s123| UP/UP| 3/A | DONE| NRML       | 0| PON   |  1|  0|
+--------------------------------------------------------------------------+
```

Step 4 **no controllers fabric plane *plane-id* shutdown**

Example:

```
sysadmin-vm: 0_RP0(config) # no controller fabric plane 3 shutdown
```

Restarts the admin plane for fabric card.

Example:

```
sysadmin-vm: 0_RP0 # commit
```

Upgrade to 400G Fabric Card Using IOS XR

This task enables the user to upgrade from a 200G fabric card (NCS4016-FC-M) to a 400G fabric card (NCS4016-FC2-M). Mixed mode (where 200G and 400G fabric cards co-exist) is recommended only while performing the upgrade. The user is required to upgrade all the FCs to 400G before making any configuration change(s).

Before you begin

The prerequisites before starting with the upgrade procedure are:

- Check for error-free traffic for at least five minutes.
- Verify the status of all the planes using the **show controller fabric plane all** command; the administration and the operational states should be displayed as **UP**.

```
sysadmin-vm:0_RP0# show controller fabric plane all
Mon Mar  14 06:50:33.720 UTC

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
```

Procedure

Step 1 **admin**

Enters the administration mode.

Step 2 **config**

Enters the configuration mode.

Step 3 **controller fabric plane** *plane-id*

Example:

```
sysadmin-vm:0_RP0(config) # controller fabric plane 0
```

Checks the current state of the fabric plane. The fabric plane of the desired card needs to be shutdown before the upgrade. For example, if the selected FC is FC0, plane 0 needs to be shutdown.

Step 4 **shutdown**

Example:

```
sysadmin-vm:0_RP0(config-plane-0) # shutdown
```

Shuts down the fabric plane.

Step 5 **commit**

Step 6 **hw-module shutdown location** *card-location*

Example:

```
sysadmin-vm:0_RP0(config) # hw-module shutdown location 0/FC0
```

Powers down the card.

Note It is mandatory to use the **commit** command after this step to power down the card.

Step 7 **commit**

Step 8 Remove the existing 200G FC and replace it with a 400G FC.

Step 9 **no hw-module shutdown location** *card-location*

Example:

```
sysadmin-vm:0_RP0(config) #  no hw-module shutdown location 0/FC0
```

Powers on the card.

Note It is mandatory to use the **commit** command after this step to power on the card.

Step 10 **commit**

Step 11 **exit**

Exits the configuration mode.

Step 12 **show platform**

Example:

```
sysadmin-vm:0_RP0 # show platform
```

Verify that the newly inserted FC is in operational state.

```
Location Card Type     HW State    SW State Config State
----------------------------------------------------------------------------
0/0      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
0/1      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
0/2      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
0/3      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
0/4      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
```

```
0/5      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
0/6      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
0/7      NCS4K-20T-O-S OPERATIONAL N/A      NSHUT
0/8      NCS4K-24LR-O-S OPERATIONAL N/A     NSHUT
0/9      NCS4K-24LR-O-S OPERATIONAL N/A     NSHUT
0/10     NCS4K-2H-O-K OPERATIONAL   N/A     NSHUT
0/11     NCS4K-2H-O-K OPERATIONAL   N/A     NSHUT
0/12     NCS4K-2H10T-OP-KS OPERATIONAL N/A  NSHUT
0/13     NCS4K-2H10T-OP-KS OPERATIONAL N/A  NSHUT
0/14     NCS4K-2H10T-OP-KS OPERATIONAL N/A  NSHUT
0/15     NCS4K-2H10T-OP-KS OPERATIONAL N/A  NSHUT
0/RP0    NCS4K-RP OPERATIONAL OPERATIONAL   NSHUT
0/RP1    NCS4K-RP OPERATIONAL OPERATIONAL   NSHUT
0/FC0    NCS4016-FC2-M OPERATIONAL    N/A   NSHUT
0/FC1    NCS4016-FC2-M OPERATIONAL    N/A   NSHUT
0/FC2    NCS4016-FC2-M OPERATIONAL    N/A   NSHUT
0/FC3    NCS4016-FC2-M OPERATIONAL    N/A   NSHUT
0/CI0    NCS4K-CRAFT OPERATIONAL      N/A   NSHUT
0/FT0    NCS4K-FTA OPERATIONAL        N/A   NSHUT
0/FT1    NCS4K-FTA OPERATIONAL        N/A   NSHUT
0/PT1    NCS4K-AC-PEM OPERATIONAL     N/A   NSHUT
0/EC0    NCS4K-ECU OPERATIONAL        N/A   NSHUT

For a specific FC, we can use:
show platform | include 0/FC0

0/FC0 NCS4016-FC2-M OPERATIONAL N/A NSHUT
```

Step 13 **show hw-module location** *location* **fpd**

Example:

```
 sysadmin-vm:0_RP0 # show hw-module location 0/FC0 fpd
```

Verify to check the status of the FPDs.

```
FPD Versions
===============
Location Card type  HWver FPD device ATR Status Run Programd
------------------------------------------------------------------------------
0/FC0 NCS4016-FC2-M 0.1 CCC-FPGA     NEED UPGD 1.12 1.12
0/FC0 NCS4016-FC2-M 0.1 CCC-Power-On CURRENT   1.01 1.01
0/FC0 NCS4016-FC2-M 0.1 PLX-8649     CURRENT 0.08 0.08
```

Note The **NEED UPGD** keyword in the Status column indicates that an FPD upgrade is required. To update an FPD, use the **upgrade hw-module location** *location* **fpd** *fpd-name* command.

Step 14 **config**

Enters the configuration mode.

Step 15 **controller fabric plane** *plane-id*

Example:

```
sysadmin-vm:0_RP0 (config) # controller fabric plane 0
```

Allows the user to perform further configurations on the selected plane.

Step 16 **no shutdown**

Example:

```
sysadmin-vm:0_RP0(config-plane-0) # no shutdown
```

Brings up the fabric plane again.

Step 17 **commit**

Step 18 **exit**

Exits the configuration mode.

Step 19 **show controller fabric plane all**

Example:

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

Verification to check if the fabric plane status is displayed as **UP**.

What to do next

Repeat the above procedure to upgrade the remaining fabric cards.

Daisy Chain on Management Ports

Table 24: Feature History

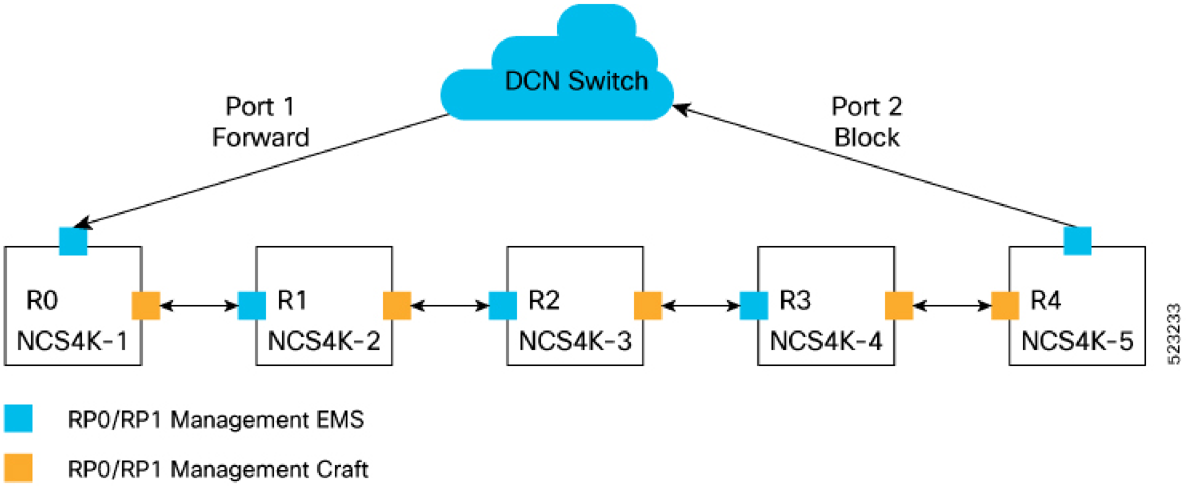
Feature Name	Release Information	Description
Daisy Chain Support on NCS 4000	Cisco IOS XR Release 6.5.33	Typically the NCS 4000 devices are connected to a switch requiring 1-to-1 connections. From this release, it will be possible to have a Daisy Chain topology. Here multiple NCS 4000 devices are connected to form a chain-like structure, and only the first and last nodes are connected to a switch, thereby reducing the number of connections. Also, there is more redundancy as data is transmitted in both directions. The first connection acts as a primary path and carries the traffic whereas the last connection acts as a backup path. If the primary connection fails, the backup path is activated which allows traffic to continue to transmit in the network.

The daisy chain arrangement allows multiple NCS 4000 nodes to be connected to each other in a ring, where the first and last nodes are connected to a switch. The switch allows management of all the NCS4000 devices in the network and also prevents traffic storm. This arrangement allows the switch to transmit data in both directions and prevents one node failure from cutting off certain network parts.

Note When the EMS or Craft management interface is administratively shutdown using the **shutdown** command, the peer router interface does not go down due to HW limitation.

The following diagram shows the Daisy Chain topology where five NCS 4000 nodes are connected to each other over the EMS and CRAFT management ports.

Figure 4: NCS4K in a Daisy Chain Network



Configuring Daisy Chain on NCS 4000 involves the following tasks:

Configure Daisy Chain on Switch

You must configure the switch by connecting the switch ports to the head and tail nodes of the NCS4K device before configuring all the NCS4K devices in a daisy chain network. To configure Daisy Chain on switch, follow these steps:

Before you begin

The following prerequisites must be met before configuring Daisy chain on NCS4000:

- Enable Storm Control on Switch.
- STP must be running on the TOR switch.
- Management port 0 must not be in shut down state and must be configured with either IPv4 address.
- Management port 1 must not be configured with IP address.
- Daisy chain must be enabled on all the NCS4000 devices in the topology.

Procedure

Step 1 To connect the port 1/0/1 of the switch with the head node of the NCS4K device, perform these steps:

a) **interface** *type* **Rack/Slot/Instance/Port**

Example:

```
RP/0/RP0:switch(config)# interface gigabitethernet 0/1/0/1
```

Sets 0/1/0/1 as Gigabit Ethernet port and enters the port configuration mode.

b) **switchport access vlan** *vlan-id*

Example:

```
RP/0/RP0:switch(config)# switchport access vlan 1526
```

Configures the VLAN id 1526 for which this access port carries the traffic.

c) **switchport mode** *mode*

Example:

```
RP/0/RP0:switch(config)# switchport mode access
```

Specifies the Ethernet port as an access port.

Step 2 To connect the port 1/0/2 of the switch with the tail node of the NCS4K device, perform these steps:

a) **interface** *type* **Rack/Slot/Instance/Port**

Example:

```
RP/0/RP0:switch(config)# interface gigabitethernet 0/1/0/2
```

Sets 0/1/0/2 as Gigabit Ethernet port and enters the interface configuration mode.

b) **switchport access vlan** *vlan-id*

Example:

```
RP/0/RP0:switch(config)# switchport access vlan 1526
```

Configures the VLAN id 1526 for which this access port carries the traffic.

c) **switchport mode** *mode*

Example:

```
RP/0/RP0:switch(config)# switchport mode access
```

Specifies the Ethernet port as an access port.

Step 3 To configure the management ports, perform these steps:

a) **interface** *type* **Rack/Slot/Instance/Port**

Example:

```
RP/0/RP0:switch(config)# interface gigabitethernet 0/1/0/24
```

Sets 0/1/0/24 as Gigabit Ethernet port and enters the interface configuration mode.

b) **switchport access vlan** *vlan-id*

Example:

```
RP/0/RP0:switch(config)# switchport access vlan 1526
```

Configures the VLAN id 1526 for which this access port carries the traffic.

Step 4 To configure the vlan port, perform these steps:

a) **interface** *type* **Rack/Slot/Instance/Port**

Example:

```
RP/0/RP0:switch(config)# interface vlan 1526
```

Sets 1526 as VLAN port and enters the interface configuration mode.

b) **ip address** *addresssubnet-mask*

Example:

```
RP/0/RP0:switch(config)# ip address 10.0.24.32 255.255.255.224
```

Configures the ip address 10.0.24.32 on the CRAFT port of the head node.

For more details about these commands, see the Cisco Nexus 9000 Series NX-OS Command Reference guide.

Configure Daisy Chain on NCS 4000

After configuring Daisy Chain on switch, you need to configure daisy chain on the NCS 4000 devices. To configure Daisy Chain on NCS 4000, follow these steps:

Procedure

Step 1 To assign IP address to the EMS port of slot RP0, perform these steps:

a) **interface** *type* **Rack/Slot/Instance/Port**

Example:

```
RP/10/RP0:ios(config)#interface MgmtEth0/RP0/EMS/0
```

b) **no shutdown**

Example:

```
RP/10/RP0:ios(config-if)#no shut
```

c) **ipv4 address odu**

Example:

```
RP/10/RP0:ios(config-if)#ipv4 address 192.168.1.12/16
```

Step 2 To configure the CRAFT port of slot RP0, perform these steps:

a) **interface** *type* **Rack/Slot/Instance/Port**

Example:

```
RP/0/RP0:Node-41(config)#interface  MgmtEth0/RP0/CRAFT/0
```

b) **bridge-port routed-interface** *type***Rack/Slot/Instance/Port**

Example:

```
RP/0/RP0:Node-41(config-if)#bridge-port routed-interface MgmtEth0/RP0/EMS/0
```

c) **no shutdown**

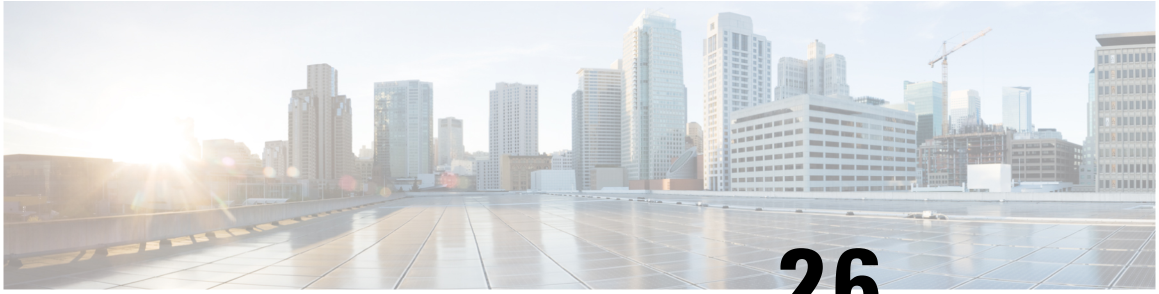
Example:

```
RP/0/RP0:Node-41(config-if)#no shutdown
```

Step 3 To assign IP address to the EMS port of slot RP1, perform the step 1.

Step 4 To configure the CRAFT port of slot RP1, perform the step 2.

For more details about these commands, see the Daisy Chain Network Command Reference section of Command Reference for Cisco NCS 4000 Series guide.



CHAPTER 26

Configure the OTN Circuits

This chapter describes the OTN circuits and procedures to configure the OTN circuits.

Create a GMPLS UNI Circuit

Before you begin

Configure refresh optical interval. See Configure the Refresh Optical Interval, on page 266.

Configure loopback interface. See Provision Loopback Interface, on page 80.

Configure the OSPF on an interface . See Configure the OSPF on an Interface, on page 263.

Configure the MPLS-TE on an OTN Controller. See Configure the MPLS-TE on an OTN Controller, on page 267.

Procedure

Step 1 **configure**

Step 2 **lmp {gmpls | port | trace} optical-uni {controller | neighbor | router-id}** *controller-name R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# lmp gmpls optical-uni controller optics 0/0/0/4
```

Enters the LMP GMPLS UNI controller configuration mode. The value of lmp port ranges from 1 to 65535.

Step 3 **neighbor** *name*

Example:

```
RP/0/RP0:hostname (config-lmp-gmpls-uni-cntl)# neighbor xr4
```

Configures the LMP neighbor name of a controller.

Step 4 **neighbor interface-id unnumbered** *value*

Example:

```
RP/0/RP0:hostname (config-lmp-gmpls-uni-cntl)# neighbor interface-id unnumbered 4
```

Configures the interface identifier for the LMP. The value of interface-ID ranges from 1 to 4294967295.

Step 5 **neighbor link-id ipv4 unicast** *address*

Example:

```
RP/0/RP0:hostname (config-lmp-gmpls-uni-cntl)# neighbor link-id ipv4 unicast 1.2.2.4
```

Configures the LMP neighbor link identifier address.

Step 6 **link-id ipv4 unicast** *value*

Example:

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

Configures the LMP GMPLS UNI link identifier address.

Step 7 **exit**

Example:

```
RP/0/RP0:hostname (config-lmp-gmpls-uni-cntl)# exit
```

Exits the LMP GMPLS UNI controller configuration mode.

Step 8 **lmp {gmpls | port | trace} optical-uni neighbor** *name*

Example:

```
RP/0/RP0:hostname (config)# lmp gmpls optical-uni neighbor xr4
```

Enters the LMP GMPLS UNI neighbor mode.

Step 9 **ipcc routed**

Example:

```
RP/0/RP0:hostname (config-lmp-gmpls-uni-nbr-xr4)# ipcc routed
```

Configures a GMPLS UNI LMP neighbor and create a routed IPCC.

Step 10 **router-id ipv4 unicast** *value*

Example:

```
RP/0/RP0:hostname (config-lmp-gmpls-uni-nbr-xr4)# router-id ipv4 unicast 1.1.1.1
```

Configures a router id for UNI LMP.

Step 11 **exit**

Example:

```
RP/0/RP0:hostname (config-lmp-gmpls-uni-nbr-xr4)# exit
```

Exits the LMP GMPLS UNI neighbor mode.

Step 12 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config)# mpls traffic-eng
```

Enters the MPLS traffic-eng configuration mode.

Step 13 **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** *head node IP address*

Note This step is applicable only when a diverse circuit is created.

Example:

```
RP/0/RP0:hostname (config)# attribute-set xro Xro_uni1_tun1_div_tun0
exclude strict lsp source 10.77.142.75 destination 10.77.142.71 tunnel-id 0 extended-tunnel-id
 10.77.142.75
```

Defines an attribute set for creating diverse circuit of a circuit with head node IP : 10.77.142.75, tail node IP:10.77.142.71 and tunnel id :0.

Note The source, destination, tunnel-id and extended-tunnel-id is the information of the circuit whose diverse circuit you want to create.

Step 14 **gmpls optical-uni controller** *controller-name R/S/I/P*

Example:

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

Enters the GMPLS UNI controller configuration mode.

Step 15 **tunnel-properties tunnel-id** *value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-cntl)# tunnel-properties tunnel-id 6
```

Configures the GMPLS-UNI tunnel ID. The value of tunnel-ID ranges from 0 to 64535.

Step 16 **tunnel-properties destination ipv4 unicast** *value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-cntl)# tunnel-properties destination ipv4 unicast 1.2.3.4
```

Specifies the GMPLS-UNI tunnel destination.

Step 17 **tunnel-properties path-option 1 no-ero [xro-attribute-set] lockdown**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-cntl)# tunnel-properties path-option 1 no-ero lockdown

RP/0/RP0:hostname (config-te-gmpls-cntl)# tunnel-properties path-option 1 no-ero
xro-attribute-set Xro_uni1_tun1_div_tun0 lockdown

RP/0/RP0:hostname (config-te-gmpls-cntl)# tunnel-properties path-option 1 explicit name
Explicit_path_tun100 lockdown verbatim
```

Configures the GMPLS-UNI path-option.

Step 18 **exit**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-cntl)# exit
```

Exits the GMPLS UNI controller configuration mode.

Step 19 **commit**

Example: Create a GMPLS-UNI Circuit

This example shows how to create a GMPLS-UNI circuit using Cisco IOS XR commands:

```
RP/0/RP0:hostname(config)# lmp gmpls optical-uni controller optics 0/0/0/4
RP/0/RP0:hostname(config-lmp-gmpls-uni-cntl)# neighbor xr4
RP/0/RP0:hostname(config-lmp-gmpls-uni-cntl)# neighbor link-id ipv4 unicast 1.2.3.4
RP/0/RP0:hostname(config-lmp-gmpls-uni-cntl)# neighbor interface-id unnumbered 4
RP/0/RP0:hostname(config-lmp-gmpls-uni-cntl)# link-id ipv4 unicast 1.2.3.4
RP/0/RP0:hostname(config-lmp-gmpls-uni-cntl)# exit
RP/0/RP0:hostname(config-lmp-gmpls-uni)# exit
RP/0/RP0:hostname(config-lmp)# exit
RP/0/RP0:hostname(config)# lmp gmpls optical-uni neighbor xr4
RP/0/RP0:hostname(config-lmp-gmpls-uni-nbr-xr4)# ipcc routed
RP/0/RP0:hostname(config-lmp-gmpls-uni-nbr-xr4)# router-id ipv4 unicast 1.1.1.1
RP/0/RP0:hostname(config-lmp-gmpls-uni-nbr-xr4)# exit
RP/0/RP0:hostname(config-lmp-gmpls-uni)# exit
RP/0/RP0:hostname(config-lmp)# exit
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 6
RP/0/RP0:hostname(config-te-gmpls-cntl)# tunnel-properties destination ipv4 unicast 1.2.3.4
RP/0/RP0:hostname(config-te-gmpls-cntl)# tunnel-properties path-option 10 no-ero lockdown
RP/0/RP0:hostname(config-te-gmpls-cntl)# exit
RP/0/RP0:hostname(config-te-gmpls-uni)# exit
RP/0/RP0:hostname(config-mpls-te)# exit
```

What to do next

Create an OTN Controller. Configure an OTN Controller, on page 228

Provision Loopback Interface

Purpose	This procedure provisions the loopback interface
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Software I
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click the **Provisioning** > **Network** > **Loopback IF** tabs.

Step 2 If you want to create a loopback interface, complete the following:

- Click **Create**. The Create Loopback Interface dialog box appears.

- Enter the Interface ID, IP address, and network mask in the respective fields and click **OK**.

Step 3 If you want to edit a loopback interface, complete the following:

- Click **Edit**. The Edit Loopback Interface dialog box appears.
- Modify the values of the IP Address and network mask as required and click **OK**.

Step 4 Return to your originating procedure.

Configure the OSPF on an Interface

Before you begin

Optics controller should be created before configuring OSPF on an interface.

Procedure

Step 1 **configure**

Step 2 **router ospf** *name-of-the-process*

Example:

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

Enables OSPF routing and enters OSPF configuration mode.

Step 3 **router-id** *id-of-the-router*

Example:

```
RP/0/RP0:hostname (config-ospf)# router-id 2.2.2.2
```

Specifies the OSPF router ID. The identifier is in the IPv4 address format.

Step 4 **area** *id-of-the-area*

Example:

```
RP/0/RP0:hostname (config)# area 4
```

Specifies the OSPF area ID and enters the area configuration mode. The identifier can be either a decimal value or an IPv4 address. The OSPF area ID value ranges from 0 to 4294967295.

Step 5 **interface loopback** *id*

Example:

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

Configures OSPF on the specified interface.

Step 6 **interface gcc0** *R/S/I/P*

Example:

```
RP/0/RP0:hostname (config-ospf-ar)# interface interface gcC0 0/1/0/1
```

Configures OSPF on the specified interface.

Step 7 **commit**

Example: Configure OSPF on an Interface

The following example shows how to configure OSPF on an interface using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# router ospf abc
RP/0/RP0:hostname(config-ospf)# router-id 2.2.2.2
RP/0/RP0:hostname(config)# area 4
RP/0/RP0:hostname(config-ospf-ar)# interface gcc0 0/0/0/4
RP/0/RP0:hostname(config-ospf-ar)# exit
```

Configure the OSPF-TE on an Interface

Before you begin

Optics controller should be created before configuring the OSPF-TE on an interface.

Procedure

Step 1 **configure**

Step 2 **router ospf** *name-of-the-process*

Example:

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

Enables OSPF routing and enters OSPF configuration mode.

Step 3 **router-id** *id-of-the-router*

Example:

```
RP/0/RP0:hostname (config-ospf)# router-id 1.1.1.1
```

Specifies the OSPF router ID. The identifier is in the IPv4 address format.

Step 4 **area** *id-of-the-area*

Example:

```
RP/0/RP0:hostname (config-ospf)# area 6
```

Specifies the OSPF area ID and enters the area configuration mode. The identifier can be either a decimal value or an IPv4 address. The OSPF area ID value ranges from 0 to 4294967295.

Step 5 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config-ospf-ar)# mpls traffic-eng
```

Enables GMPLS for the specified OSPF-TE area.

Step 6 **interface loopback** *range-of-the-interface loopback*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface loopback 5
```

Creates a loopback interface for the specified OSPF-TE area and enters the loopback interface configuration mode. The interface loopback value ranges from 0 to 65535.

Step 7 **passive [disable | enable]**

Example:

```
RP/0/RP0:hostname (config-ospf-ar-if)# passive enable
```

Specifies that the OSPF-TE configuration is passive.

Step 8 **exit**

Example:

```
RP/0/RP0:hostname (config-ospf-ar-if)# exit
```

Exits the loopback interface configuration mode.

Step 9 **interface GCC0** *R/S/I/P*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface GCC0 0/0/0/20
```

Enables GCC on the interface and enters the OSPF-TE interface configuration mode.

Step 10 **exit**

Example:

```
RP/0/RP0:hostname (config-ospf-ar)# exit
```

Exits the loopback interface configuration mode.

Step 11 **mpls traffic-eng router-id loopback** *value*

Example:

```
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng router-id loopback 4
```

Enables GMPLS traffic on the loopback interface. The loopback value ranges from 0 to 65535.

Step 12 **commit**

Example: Configure OSPF-TE on an Interface

The following example shows how to configure OSPF-TE on an interface using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# router ospf abc
RP/0/RP0:hostname(config-ospf)# router-id 1.1.1.1
RP/0/RP0:hostname(config-ospf)# area 6
RP/0/RP0:hostname(config-ospf-ar)# mpls traffic-eng
RP/0/RP0:hostname(config-ospf-ar)# interface loopback 5
RP/0/RP0:hostname(config-ospf-ar-if)# passive enable
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# interface GCC0 0/0/0/20
RP/0/RP0:hostname(config-ospf-ar)# exit
```

```
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng router-id loopback 4
RP/0/RP0:hostname(config-ospf)# exit
```

Configure the Refresh Optical Interval

Before you begin

Optics controller should be created before configuring the refresh optical interval.

Procedure

Step 1 **configure**

Step 2 **rsvp**

Example:

```
RP/0/RP0:hostname(config)# rsvp
```

Enters the RSVP mode.

Step 3 **controller** *Type-of-the-controller R/S/I/P*

Example:

```
RP/0/RP0:hostname(config-rsvp)# controller otu4 0/0/0/20
```

Enters the otu4 controller mode.

Step 4 **signalling refresh out-of-band [missed | interval]** *value*

Example:

```
RP/0/RP0:hostname(config-rsvp-cntl)# signalling refresh out-of-band missed 24
```

Specifies the interval between successive refreshes. The value of missed messages ranges from 1 to 110000 and refresh interval value ranges from 180 to 86400 seconds.

Step 5 **commit**

Example: Configure Refresh Optical Interval

The following example shows how to configure refresh optical interval using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# rsvp
RP/0/RP0:hostname(config-rsvp)# controller otu4 0/0/0/20
RP/0/RP0:hostname(config-rsvp-cntl)# signalling refresh out-of-band missed 24
RP/0/RP0:hostname(config-rsvp-cntl)# exit
```

Configure the MPLS-TE on an OTN Controller

Before you begin

Optics controller should be created before configuring mpls-te on an otn controller.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config)# mpls traffic-eng
```

Enters the MPLS-TE configuration mode.

Step 3 **gmpls [nni | optical-uni]**

Example:

```
RP/0/RP0:hostname (config-mpls-te)# gmpls nni
```

Enters the GMPLS Interface configuration mode. You can specify two types of interface: UNI and NNI.

Step 4 **topology instance ospf** *name-of-the-topology instance* **area***value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni)# topology instance ospf abc area 5
```

Configures the topology instance of the OSPF. The value of OSPF area ID ranges from 0 to 4294967295.

Step 5 **controller** *name-of-the-controller R/S/I/P*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni-ti)# controller otu4 0/0/0/1
```

Configures the GMPLS-NNI on the specified OTN controller.

Step 6 **admin-weight** *value-of-the-admin-weight*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni-ti-cntl)# admin-weight 7
```

Configures admin weight on the specified controller. The valid range is from 0 to 65535.

Step 7 **commit**

Example: Configure MPLS-TE on an OTN Controller

The following example shows how to configure MPLS-TE on an OTN controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)#  mpls traffic-eng
```

```
RP/0/RP0:hostname(config-mpls-te)#  gmpls nni
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)#  admin-weight 7
RP/0/RP0:hostname(config-line)# exit
```

Create an OTN Circuit through Control Plane

Before you begin

Optics controller should be created before creating an otn circuit.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config)# mpls traffic-eng
```

Enters the MPLS traffic-eng configuration mode.

Step 3 **gmpls nni**

Example:

```
RP/0/RP0:hostname (config-mpls-te)# gmpls optical-nni
```

Enters the GMPLS NNI configuration mode.

Step 4 **controller odu-group-te** *tunnel-ID*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni)# controller Odu-Group-Te 7
```

Enters the Odu-Group-Te configuration mode. The tunnel ID value ranges from 0 to 63535.

Step 5 **destination** *type-of-the-destination* **unicast** *address-of-the-destination*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# destination ipv4 unicast 2.2.2.2
```

Specifies the destination IPv4 unicast address.

Step 6 **static-uni ingress-port controller** *name-of-the-controller R/S/I/P* **egress-port unnumbered** *value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# static-uni ingress-port controller
GigabitEthernet 0/0/0/3 egress-port unnumbered 6
```

Sets the static UNI endpoints of the NNI tunnel. The port IF index value ranges from 0 to 4294967295.

Step 7 **signalled-bandwidth** *type-of-the-controller*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# signalled-bandwidth odu1
```

Sets the signal bandwidth of the controller.

Step 8 **signalled-name** *name*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# signalled-name abcd
```

Specifies the signalled name for signalling. The maximum length is 64 characters.

Step 9 **path-protection attribute-set** *name-of-the-attribute-set*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-protection attribute-set ss
```

Specifies the attribute set name for path protection. The maximum length is 32 characters.

Step 10 **path-option** *value* **[dynamic | explicit] [lockdown | protected-by | restored-from]** *preference level-of-the-path-option* **[lockdown | restored-from]** *preference level-of-the-path-option* **lockdown**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-option 5 dynamic protected-by 10
restored-from 30 lockdown
```

Configures the setup type and preference level of path option. The range of preference value is from 1 to 1000.

Note You can modify a path option once you have created it.

Step 11 **logging events lsp-status state**

Example:

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

Enables the interface lsp state alarms.

Step 12 **commit**

Example: Create an OTN Circuit

The following example shows how to create an explicit path using Cisco IOS XR commands:

```
RP/0/RP0:hostname # configure terminal
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 7
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# destination ipv4 unicast 2.2.2.2
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# static-uni ingress-port controller
GigabitEthernet 0/0/0/3 egress-port unnumbered 6
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# signalled-bandwidth odu1
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# signalled-name abcd
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-protection attribute-set ss
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-option 5 dynamic protected-by 10
restored-from 30 lockdown
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# logging events lsp-status state
RP/0/RP0:hostname # commit
```

Configure a Permanent Connection (xconnect)

Before you begin

Optics controller should be created before configuring a permanent connection.

Procedure

Step 1 **configure**

Step 2 **xconnect** *ID-of-the-xconnect* **endpoint-1** *Type-of-the-controller R/S/I/P* **endpoint-2** *Type-of-the-controller R/S/I/P*

Example:

```
RP/0/RP0:hostname(config)# xconnect 5 endpoint-1 ODU1 0/0/0/2 endpoint-2 ODU1 0/0/0/2
```

Configures a permanent connection between two ODUk controllers. The cross connection ID value ranges from 1 to 32655

Note A cross connection can only be made between same type of controllers such as ODU1-ODU1 and ODU2-ODU2.

Step 3 **commit**

View a Permanent Connections

Before you begin

Create a permanent connection. See Configure a Permanent Connection (xconnect), on page 270.

Procedure

Step 1 **configure**

Step 2 **show xconnect [all | id | trace]**

Example:

```
RP/0/RP0:hostname# show xconnect all
```

Displays details of all the permanent connections.

Step 3 **show xconnect [all | id | trace]** *ID-value*

Example:

```
RP/0/RP0:hostname# show xconnect id 5
```

Displays details of all the permanent connections for the given connection ID. The cross connection ID value ranges from 1 to 32655.

Step 4 **commit**

Create a GMPLS NNI Circuit

Before you begin

Configure loopback interface. See Provision Loopback Interface, on page 80.

Configure the OSPF on an interface . See Configure the OSPF on an Interface, on page 263.

Configure the MPLS-TE on an OTN Controller. See Configure the MPLS-TE on an OTN Controller, on page 267.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config)# mpls traffic-eng
```

Enters the MPLS traffic-eng configuration mode.

Step 3 **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** *head node IP address*

Note This step is applicable only when a diverse circuit is created.

Example:

```
RP/0/RP0:hostname (config)# attribute-set xro Xro_nni1_tun1_div_tun0
exclude strict lsp source 10.77.142.75 destination 10.77.142.71 tunnel-id 0 extended-tunnel-id
 10.77.142.75
```

Defines an attribute set for creating diverse circuit of a circuit with head node IP : 10.77.142.75, tail node IP:10.77.142.71 and tunnel id :0.

Note The source, destination, tunnel-id and extended-tunnel-id is the information of the circuit whose diverse circuit you want to create.

Step 4 **gmpls optical-nni controller** *controller-name R/S/I/P*

Example:

```
RP/0/RP0:hostname (config-mpls-te)# gmpls optical-nni controller Odu-Group-te 17
```

Enters the GMPLS-NNI controller configuration mode.

Step 5 **destination ipv4 unicast** *value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11)# destination ipv4 unicast 1.2.3.4
```

Specifies the GMPLS-NNI tunnel destination.

Step 6 **signalled-bandwidth ODU1**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11# signalled-bandwidth ODU1
```

Specifies the signalled bandwidth.

Step 7 **path-option 1 dynamic protected-by** *value* **[xro-attribute-set]** *xro attribute set name* **lockdown**

Note Use xro-attribute-set option only for creating a diverse circuit.

protected-by value is always set to none as only protection type 1+0 is supported with circuit diversity.

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11)# path-option 1 dynamic protected-by 2 lockdown
```

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11)# path-option 1 dynamic protected-by none
xro-attribute-set Xro_uni1_tun1_div_tun0 lockdown
```

Configures the GMPLS-NNI path-option.

Step 8 **path-option 2 dynamic lockdown**

Note This step is not applicable for creating a diverse circuit.

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11)# path-option 2 dynamic lockdown
```

Configures the GMPLS-NNI path-option.

Step 9 **path-protection attribute-set** *value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11)# path-protection attribute-set attSet1
```

Configures the GMPLS-NNI path-protection.

Step 10 **static-uni ingress-portcontroller otu1** *R/S/I/P* **egress-port unnumbered** *value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11)# static-uni ingress-port controller otu1
0/1/0/20 egress-port unnumbered 56
```

Configures the interface identifier for the LMP. The value of interface-ID ranges from 1 to 4294967295.

Step 11 **exit**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x11)# exit
```

Exits the GMPLS UNI controller configuration mode.

Step 12 **commit**

Example: Create a GMPLS NNI Circuit

This example shows how to create a GMPLS NNI circuit using Cisco IOS XR commands:

```
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni controller Odu-Group-te 17
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# destination ipv4 unicast 1.2.3.4
```

```
RP/0/RP0:hostname(config-te-gmpls-tun-0x11# signalled-bandwidth ODU1
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# path-option 1 dynamic protected-by 2 lockdown
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# path-option 2 dynamic lockdown
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# path-protection attribute-set soumya
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# static-uni ingress-port controller otu1 0/1/0/20
 egress-port unnumbered 56
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# exit
```

What to do next

Create an OTN Controller. See Configure an OTN Controller, on page 228.

Configure the MPLS-TE on an OTN Controller using Local Termination

Before you begin

Optics controller should be created before configuring mpls-te on an otn controller.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config)# mpls traffic-eng
```

Enters the MPLS-TE configuration mode.

Step 3 **gmpls optical-nni**

Example:

```
RP/0/RP0:hostname (config-mpls-te)# gmpls optical-nni
```

Enters the GMPLS Interface configuration mode.

Step 4 **topology instance ospf** *name-of-the-ospf instance* **area***value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni)# topology instance OTN abc area 0
```

Configures the topology instance of the OSPF. The value of OSPF area ID ranges from 0 to 4294967295.

Step 5 **controller** *name-of-the-controller R/S/I/P*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni-ti)# controller otu4 0/1/0/1
```

Configures the GMPLS-NNI on the specified OTN controller.

Step 6 **tti-mode** *mode*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni-ti-cntl)# tti-mode otu-sm
```

Step 7 **admin-weight** *value-of-the-admin-weight*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni-ti-cntl)# admin-weight 1
```

Configures admin weight on the specified controller. The valid range is from 0 to 65535.

Step 8 **exit**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni-ti-cntl)# exit
```

Exits the current sub mode.

Step 9 **exit**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni-ti)# exit
```

Exits the current sub mode.

Step 10 **exit**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni)# exit
```

Exits the current sub mode.

Step 11 **gmpls optical-nni controller** *controller-name R/S/I/P*

Example:

```
RP/0/RP0:hostname (config-mpls-te)# gmpls optical-nni controller Odu-Group-te 17
```

Enters the GMPLS-NNI controller configuration mode.

Step 12 **signalled-bandwidth***type-of-the-controller*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# signalled-bandwidth odu2
```

Sets the signal bandwidth of the controller.

Step 13 **static-uni local-termination interface-name** *name-of-the-interface R/S/I/P* **remote-termination unnumbered** *value*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# static-uni local-termination interface-name
TenGigE0/1/0/1/1 remote-termination unnumbered 52
```

Configures the local termination interface identifier of the controller.

Step 14 **destination** *type-of-the-destination* **unnumbered***value* **interface-ifindex** *index value*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)#destination ipv4 unnumbered 13.13.13.13
interface-ifindex 55
```

Configures the destination.

Step 15 **path-option** *value* **dynamic protected-by** *value* **lockdown**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)# path-option 1 dynamic protected-by none lockdown
```

Step 16 **commit**

Example: Configure MPLS-TE on an OTN Controller Using Local Termination

The following example shows how to configure MPLS-TE on an OTN controller using local termination method:

```
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 OTN area 0
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)# tti -mode otu-sm
RP/0/RP0:hostname(config-te-gmpls-nni-ti-cntl)#  admin-weight 1
RP/0/RP0:hostname(config-te-gmpls-nni-ti-cntl)#  exit
RP/0/RP0:hostname(config-te-gmpls-nni-ti)#  exit
RP/0/RP0:hostname(config-te-gmpls-nni)#  exit
RP/0/RP0:hostname (config-mpls-te)#  gmpls optical-nni controller Odu-Group-te 17
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)#  signalled -bandwidth odu2
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)#  static -uni local-termination interface-name
 TenGigE0/1/0/1/1 remote-termination unnumbered 52
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)#  destination ipv4 unnumbered 13.13.13.13
interface- ifindex 55
RP/0/RP0:hostname(config-te-gmpls-tun-0x11)#path-option 1 dynamic protected-by none lockdown
```

OCH Mutual Circuit Diversity

The OCH Mutual Circuit Diversity feature is an interoperability feature between a NCS 4000 series router and a NCS 2000 series router.

This feature enables the user to create two separate circuits whose paths use a different set of nodes.

Consider a DWDM circuit carrying a service. In order to provide protection and reduce the probability of simultaneous connection failures, the user can create a new circuit by defining a different set of nodes. In case of failure, the service is seamlessly carried forward by the other circuit, which has a different path. Typically, nodes dynamically choose the shortest path, where a circuit is created to reach the destination using minimum number of hops. This might result in network congestion if the same nodes are used by many circuits. Mutual circuit diversity enables the user to allocate different network paths for two circuits. Both the circuits are defined in such a way that there are no overlapping nodes (except the source node), and the paths are independent of each other.

This feature is supported on DWDM-enabled optical ports for the following cards:

- NCS4K-2H10T-OP-KS – port 2 to 11 when equipped with SFP+ with PID ONS-SC+-10G-C
- NCS4K-2H-W – trunk ports 2 and 3
- NCS4K-4H-OPW-QC2 – trunks ports 10 and 11

Configuring Mutual Circuit Diversity - Overview of tasks

The following are the pre-requisites required to configure mutual circuit diversity (the user can use CTC to configure the following):

- Configure Link Management Protocol between the NCS 4000 and NCS 2000 nodes, refer Create an LMP Using CTC, on page 93
- Enable Refresh Optical Interval (RSVP), refer Configure a RSVP-TE Instance Using CTC, on page 78

For configuring mutual diversity, the attributes are set for two circuits. Diverse paths are explicitly defined for both the circuits.

- Configure GMPLS tail node configuration
- Configure explicit path
- Create OCH trail circuits with mutual diversity

Configure GMPLS tail node

This task enables the user to set up an optical unnumbered interface for the end point controllers.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config) # mpls traffic-eng
```

Enters MPLS-TE configuration mode.

Step 3 **gmpls optical-uni**

Example:

```
RP/0/RP0:hostname (config-mpls-te) # gmpls optical-uni
```

Enters the GMPLS UNI configuration submode.

Step 4 **controller optics** *interface*

Example:

```
RP/0/RP0:hostname (config-te-gmpls) # controller optics 0/1/0/2
```

Enters the GMPLS UNI controller submode for the specified interface.

Step 5 **commit**

What to do next

Define paths for circuits

Configure Explicit Path

This task enables the user to set-up the path for a circuit using strict or loose hops. Explicit path configuration is applicable to the GMPLS head node.

When a strict hop is configured, it identifies an exact path through which the circuit must be routed. When a loose hop is configured, the path can be changed.

Procedure

Step 1 **configure**

Step 2 **explicit-path name** *name*

Example:

```
RP/0/RP0:hostname(config) # explicit-path name ExplicitPath0_2_0_2to1_1_1_85_sh0_sl1_p2
```

Provides the path name.

Step 3 **index** *index-id* **next-address [strict | loose] ipv4 unicast unnumbered** *ip-address* *id*

Example:

```
RP/0/RP0:hostname (config) # index 10 next-address strict ipv4 unicast unnumbered 10.10.1.119
 2130706962
```

Configures the ingress interface.

Step 4 **index** *index-id* **next-address [strict | loose] ipv4 unicast unnumbered** *ip-address* *id*

Example:

```
RP/0/RP0:hostname (config) # index 80 next-address loose ipv4 unicast unnumbered 1.1.1.85
35
```

Configures the destination interface.

Step 5 **commit**

What to do next

Configure diversity by defining the attributes for both the circuits

Create OCH Trail Circuits with Mutual Diversity

This task enables the user to set the path attributes for a circuit. As earlier discussed, the attributes need to be defined for both the circuits and this configuration needs to be carried out twice. It is recommended to commit the configuration after setting the attributes for the second circuit, as signaling is initiated, only after the second circuit attributes are committed.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config) # mpls traffic-eng
```

Enters MPLS-TE configuration mode.

Step 3 **attribute-set xro exclude** *circuit-name*

Example:

```
RP/0/RP0:hostname (config-te) # attribute-set xro exclude CircuitB
```

Enters the attribute set submode and specifies the attribute set name. The path definition contains the circuit to be excluded.

Step 4 **exclude srict lsp source** *source ip-address* **destination** *destination ip-address* **tunnel-id** *number* **extended tunnel-id** *source ip-address*

Example:

```
RP/0/RP0:hostname (config-te-attribute-set) # exclude strict lsp source 1.1.1.83 destination
 1.1.1.63 tunnel-id 1 extended-tunnel-id 1.1.1.83
```

Sets the path diversity and defines the attributes.

Step 5 **exit**

Step 6 **gmpls optical-uni**

Example:

```
RP/0/RP0:hostname (config-mpls-te) # gmpls optical-uni
```

Enters the GMPLS UNI configuration submode.

Step 7 **controller optics** *interface*

Example:

```
RP/0/RP0:hostname (config-te-gmpls) # controller optics 0/1/0/2
```

Enters the GMPLS UNI controller submode for the specified interface.

Step 8 **announce srlgs**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-cntl)# announce srlgs
```

Announces discovered SRLGs to the system.

Step 9 **tunnel-properties**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-cntl)# tunnel-properties
```

Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.

Step 10 **signalled-name** *circuit-name*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-cntl)# signalled-name Circuit A
```

Sets the name for the circuit which needs to follow a path different from the attributes defined earlier.

Step 11 **tunnel-id** *number*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun)# tunnel-id 0
```

Specifies a tunnel-ID for a headend router of a GMPLS tunnel. The tunnel-ID is a 16-bit number ranging from 0 to 65535.

Step 12 **record srlg**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun)# record srlg
```

Enables SRLG recording.

Step 13 **destination ipv4 unicast** *address*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun)# destination ipv4 unicast 1.1.1.85
```

Specifies a tunnel destination for a headend router of a GMPLS tunnel. The destination argument is an IPv4 address.

Step 14 **path-option** *number* **explicit-path name** *name* **xro-attribute-set exclude** *attribute* **lockdown verbatim**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun)# path-option 10 explicit-path name
ExplicitPath0_2_0_2to1_1_1_85_sh0_sl1_p2 xro-attribute-set exclude CircuitB lockdown verbatim
```

The XRO attribute set is attached to the GMPLS UNI tunnel through the path option. The path-option range is 1 to 1000.

Step 15 **record-route**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-cntl)# record-route
```

Records the path taken by the circuit.

Step 16 **commit**

Example for Configuring Mutual Circuit Diversity

Let us consider two circuits, Circuit A and Circuit B, with the following parameters:

- Circuit A: Source address - 1.1.1.83; Destination address - 1.1.1.85
- Circuit B: Source address - 1.1.1.83; Destination address - 1.1.1.63

GMPLS tail node configuration

```
Circuit A
-----------
mpls traffic-eng
    gmpls optical-uni
        controller optics0/1/0/2
    !
!

Circuit B
----------
mpls traffic-eng
    gmpls optical-uni
        controller optics0/7/0/10
!
```

Explicit path configuration

```
Circuit A
----------
explicit-path name ExplicitPath0_2_0_2to1_1_1_85_sh0_sl1_p2
    index 10 next-address strict ipv4 unicast unnumbered 10.10.1.119 2130706962
    index 80 next-address loose ipv4 unicast unnumbered 1.1.1.85 35
!

Circuit B
----------
explicit-path name ExplicitPath0_15_0_10to1_1_1_63_sh0_sl7_p10
    index 10 next-address strict ipv4 unicast unnumbered 10.10.1.119 2130706964
    index 20 next-address loose ipv4 unicast unnumbered 1.1.1.63 169
!
```

Configuring mutual diversity by defining attributes for both the circuits

```
Circuit A
----------
mpls traffic-eng
    attribute-set xro exclude-CircuitB
       exclude strict lsp source 1.1.1.83 destination 1.1.1.63 tunnel-id 1 extended-tunnel-id
 1.1.1.83
    !

    gmpls optical-uni
        controller Optics0/2/0/2
            logging discovered-srlgs
            announce srlgs
            tunnel-properties
                signalled-name CircuitA
                tunnel-id 0
                record srlg
                destination ipv4 unicast 1.1.1.85
                path-option 10 explicit name ExplicitPath0_2_0_2to1_1_1_85_sh0_sl1_p2
xro-attribute-set exclude-CircuitB lockdown verbatim
                record-route
            !
        !
    !
!

Circuit B
----------
mpls traffic-eng
    attribute-set xro exclude-CircuitA
       exclude strict lsp source 1.1.1.83 destination 1.1.1.85 tunnel-id 0 extended-tunnel-id
 1.1.1.83
    !

    gmpls optical-uni
        controller Optics0/15/0/10
            logging discovered-srlgs
            announce srlgs
                tunnel-properties
                signalled-name VZO2toHUB1
                tunnel-id 1
                record srlg
                destination ipv4 unicast 1.1.1.63
                path-option 10 explicit name ExplicitPath0_15_0_10to1_1_1_63_sh0_sl7_p10
xro-attribute-set exclude-CircuitA lockdown verbatim
                record-route
            !
        !
    !
```

Configure 1+1+R

This task enables the user to define a protect path and a restore path for a working path.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng gmpls optical-nni**

Example:

```
RP/0/RP0:hostname(config) # mpls traffic-eng gmpls optical-nni
```

Enters the MPLS traffic engineering and GMPLS NNI configuration mode.

Step 3 **controller odu-group-te** *tunnel-ID*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni)# controller Odu-Group-Te 7
```

Enters the Odu-Group-Te configuration mode. The tunnel ID value ranges from 0 to 63535.

Step 4 **signalled-name** *name*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# signalled-name abcd
```

Specifies the signalling name. The maximum length is 64 characters.

Step 5 **signalled-bandwidth** *controller*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# signalled-bandwidth odu1
```

Sets the signal bandwidth of the controller.

Step 6 **static-uni ingress port controller** *controller R/S/I/P* **egress-port unnumbered** *value*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# static-uni ingress-port controller
GigabitEthernet 0/0/0/3 egress-port unnumbered 6
```

Sets the static UNI endpoints of the tunnel. The port index value ranges from 0 to 4294967295.

Step 7 **destination ipv4 unicast** *destination-address*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# destination ipv4 unicast 2.2.2.2
```

Specifies the destination IPv4 unicast address.

Step 8 **path-option** *value* [**dynamic** | **explicit**] [**protected-by** | **restored-from**] *preference-level* [**protected-by** | **restored-from** *preference-level* **lockdown**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-option 1 dynamic protected-by 2
restored-from 3 lockdown
```

Configures the path option 1; paths that will serve as the protect and restore paths are defined.

Step 9 **path-option** *value* [**dynamic** | **explicit**] [**protected-by** | **restored-from**] *preference-level* [**protected-by** | **restored-from** *preference-level* **lockdown**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-option 2 dynamic restored-from 3 lockdown
```

Configures the path option 2; restore path is defined.

Step 10 **path-option** *value* [**dynamic** | **explicit**] [**protected-by** | **restored-from**] *preference-level* [**protected-by** | **restored-from** *preference-level* **lockdown**

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-option 3 dynamic lockdown
```

Step 11 **commit**

Logical Patch Cord

A logical patch cord creates a connection between two optical ports. This is an external connection, enables the network administrator to connect the front plates of the cards.

Enabling a Logical Patch Cord

This task enables the user to create a connection between two optical ports.

Procedure

Step 1 **configure**

Step 2 **hw-module patchcord port optics** *interface* **port optics** *interface*

Example:

```
RP/0/RP0:hostname (config) # hw-module patchcord port optics 0/0/0/0 port optics 0/0/0/1
```

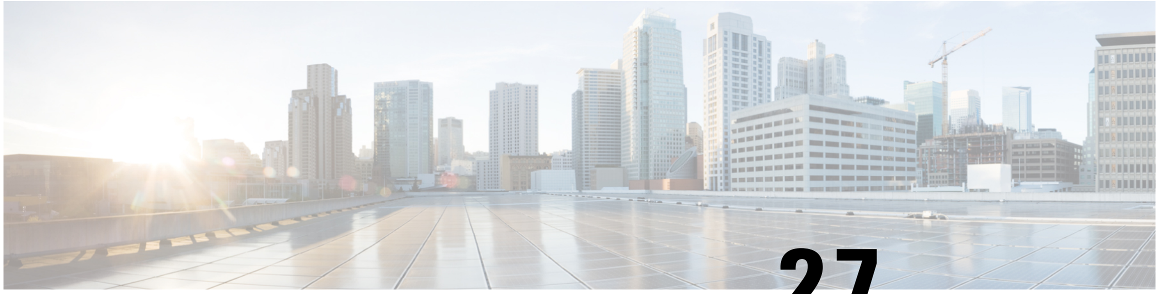
Enables connectivity between the two ports.

Step 3 **commit**

What to do next

Verify a configured patchcord:

```
show hw-module patchcord all
Hw-module Patchcord Configuration
------------------------------------------------------
Source Port             Destination Port
-------------------------------------------------------
Optics0_0_0_0           Optics0_1_0_0
```



CHAPTER 27

Configure the OTN Protection

This chapter provides the Cisco IOS XR commands to add the path protection profile and switch the traffic from working to protected path.

Define the Working and Protecting Resources in an ODU Group Controller through Management Plane

Perform this task to define the working and protecting resources in an odu group controller through management plane.

Procedure

Step 1 **configure**

Step 2 **controller odu-group-mp** *group-id-of-the-controller* **signal {Ethernet | FC | OTN | SDH | Sonet}** **odu-type** *type-of-the-odu*

Example:

```
RP/0/RP0:hostname# controller odu-group-mp 5 signal OTN odu-type odu1
```

This creates the ODU group controller. The ODU Group MP value ranges from 1 to 65535.

Step 3 **protecting-controller** *name-of-the-controller Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname (config-odu-group-mp5)# protecting-controller odu1 0/0/0/1
```

Defines an ODUk (HO/LO) controller as the protecting resource in the ODU group controller.

Step 4 **working-controller** *name-of-the-controller Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname (config-odu-group-mp5)# working-controller odu1 0/0/0/1
```

Defines an ODUk (HO/LO) controller as the working resource in the ODU group controller.

Step 5 **commit**

Example: Define Working and Protecting Resources in an ODU Group Controller

The following example defines working and protecting resources in the ODU group controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname# controller odu-group-mp 5 signal otn odu-type odu1
RP/0/RP0:hostname(config-odu-group-mp5)# protecting-controller odu1 0/0/0/1
RP/0/RP0:hostname(config-odu-group-mp5)# working-controller odu1 0/0/0/1
RP/0/RP0:hostname(config-odu-group-mp5)#exit
```

Configure the Protection Attributes of an ODU Group Controller

Perform this task to configure the protection attributes of an odu group controller.

Procedure

Step 1 **configure**

Step 2 **controller odu-group-mp** *group-id-of-the-controller* **signal {Ethernet | FC | OTN | SDH | Sonet} odu-type** *type-of-the-odu*

Example:

```
RP/0/RP0:hostname# controller odu-group-mp 5 signal OTN odu-type odu1
```

This creates the ODU group controller. The ODU Group MP value ranges from 1 to 65535.

Step 3 **protection-attributes {connection-mode | protection-mode | protection-type | timers}** *SNC mode-of-the-protection-attributes*

Example:

```
RP/0/RP0:hostname (config-odu-group-mp5)# protection-attributes connection-mode snc-i
```

Configures the connection mode of all the protecting resources in the ODU group controller. You can configure the connection mode as SNC/I, SNC/N, or SNC/S.

Step 4 **protection-attributes {connection-mode | protection-mode | protection-type | timers}** *mode-of-the-protection-attributes*

Example:

```
RP/0/RP0:hostname (config-odu-group-mp5)# protection-attributes protection-mode revertive
wait-to-restore-time 300
```

```
RP/0/RP0:hostname (config-odu-group-mp5)# protection-attributes protection-mode nonrevertive
```

Configures the protection mode of all the protecting resources in the ODU group controller. You can configure the protection mode as revertive or non revertive. The value of wait-to-restore-time ranges from 300 to 720 seconds and default value is 300 seconds.

Step 5 **protection-attributes {connection-mode | protection-mode | protection-type | timers}** *type-of-the-protection-attributes*

Example:

```
RP/0/RP0:hostname (config-odu-group-mp5)# protection-attributes protection-type APSuni
```

Configures the protection type of all the protecting resources in the ODU group controller. You can configure the protection type as 1+1 bidirectional APS, 1+1 unidirectional APS or 1+1 no APS.

Step 6 **protection-attributes {connection-mode | protection-mode | protection-type | timers} hold-off time** *timer-of-the-protection-attributes*

Example:

```
RP/0/RP0:hostname (config-odu-group-mp5)# protection-attributes timers hold-off-time 100
```

Configures hold-off timer for the ODU group controller. The valid range for the hold-off timer is from 100 to 10000 seconds.

Step 7 **commit**

Example: Configure Protection Attributes of an ODU Group Controller

The following example shows configure protection attributes of an ODU group using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname# controller odu-group-mp 5
RP/0/RP0:hostname(config-odu-group-mp5)#  protection-attributes connection-mode snc-i
RP/0/RP0:hostname(config-odu-group-mp5)#  protection-attributes protection-type APSuni
RP/0/RP0:hostname(config-odu-group-mp5)#  protection-attributes protection-mode revertive
wait-to-restore-time 300
RP/0/RP0:hostname(config-odu-group-mp5)#  protection-attributes timers hold-off-time 100
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)#  commit
```

Add a Path Protection Profile

Perform this task to add a path protection profile.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname (config)# mpls traffic-eng
```

Enters the MPLS traffic-eng configuration mode.

Step 3 **attribute-set {auto-backup | auto-mesh | p2mp-te | path-option | path-protection-aps | xro}** *name-of-the-path-protection-aps*

Example:

```
RP/0/RP0:hostname (config-mpls-te)# attribute-set path-protection-aps abc
```

Specifies the attribute set name. The maximum length for attribute set name is 32 characters.

Step 4 **sub-network connection-mode {SNC-I | SNC-N | SNC-S}**

Example:

```
RP/0/RP0:hostname (config-te-attribute-set)# sub-network connection-mode
    SNC-N
```

Specifies the sub-network connection mode.

Step 5 **protection-type {1-plus-1-BDIR-APS | a-plus-1-UNIDIR-APS | 1-plus-1-UNIDIR-NO-APS}**

Example:

```
RP/0/RP0:hostname (config-te-attribute-set)# protection-type
    1-plus-1-BDIR-APS
```

Specifies the protection type.

Step 6 **protection-mode** *mode-of-the-protection*

Example:

```
RP/0/RP0:hostname (config-te-attribute-set)# protection-mode revertive
```

Specifies the protection mode.

Step 7 **timers [hold-off | wait-to-restore]**

Example:

```
RP/0/RP0:hostname (config-te-attribute-set)# timers hold-off 350
```

Specifies the timers value in seconds. The value of hold-off timer ranges from 100 to 10000 seconds. The value for wait to restore timer ranges from 300 to 720 seconds.

Step 8 **exit**

Example:

```
RP/0/RP0:hostname (config-mpls-attribute-set)# exit
```

Exits the attribute set mode.

Step 9 **gmpls nni**

Example:

```
RP/0/RP0:hostname (config-mpls-te)# gmpls nni
```

Enters the GMPLS NNI mode.

Step 10 **controller odu-group-te** *tunnel-ID*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-nni)# controller Odu-Group-Te 7
```

Specifies the tunnel ID. The value ranges from 0 to 63535.

Step 11 **path-protection attribute-set** *name-of-the-path-protection attribute-set*

Example:

```
RP/0/RP0:hostname (config-te-gmpls-tun-0x7)# path-protection attribute-set abc1
```

Specifies the attribute set name. The maximum length for attribute set name is 32 characters.

Step 12 **commit**

Example: Add a Path Protection Profile

The following example shows how to add a path protection profile using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# attribute-set path-protection-aps abc
RP/0/RP0:hostname(config-te-attribute-set)# sub-network connection-mode SNC-N
RP/0/RP0:hostname(config-te-attribute-set)#  protection-type 1-plus-1-BDIR-APS
RP/0/RP0:hostname(config-te-attribute-set)#  protection-mode revertive
RP/0/RP0:hostname(config-te-attribute-set)#  timers hold-off 350
RP/0/RP0:hostname(config-te-attribute-set)#  exit
RP/0/RP0:hostname(config-mpls-te)#  gmpls nni
RP/0/RP0:hostname(config-te-gmpls-nni)#  controller Odu-Group-Te 7
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)#  path-protection attribute-set abc1
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)#  commit
```

Perform a Lockout

Perform this task to perform a lockout.

Procedure

Step 1 **configure**

Step 2 **controller odu-group-mp** *group id-of-the-controller*

Example:

```
RP/0/RP0:hostname(config) # controller odu-group-mp 1
```

Enters the ODU group controller mode.

Step 3 **protection-switching operate lockout odu-dest** *name-of-the-controllerRack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname (config-odu-group-mp1)# protection-switching operate lockout odu-dest
odu0 0/0/0/0
```

Configures an ODUk controller as a locked out resource in the ODU group controller.

Step 4 **commit**

Perform a Forced Switch

Perform this task to perform a forced switch.

Procedure

odu-group {mp | te} *group id-of-the-odu-group* **forced odu-dest** *name-of-the-controller Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname # odu-group mp 1 forced odu-dest odu1 0/0/0/1
```

Configures ODU0 to carry the traffic in a network.

Perform a Manual Switch

Perform this task to perform a manual switch.

Procedure

odu-group {mp | te} *group id-of-the-controller* **manual odu-dest** *name-of-the-controller Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname # odu-group mp 1 manual odu-dest odu0 0/0/0/1
```

Configures ODU0 to carry the traffic in a network. Switches the traffic manually from the working to the protected path.

CHAPTER 28

Configure SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by NCS 4000.

Prerequisites for Implementing SNMP

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.

Restrictions for SNMP Use on Cisco IOS XR Software

SNMP outputs are only 32-bits wide and therefore cannot display any information greater than 2^{32}. 2^{32} is equal to 4.29 Gigabits. Note that a 10 Gigabit interface is greater than this and so if you are trying to display speed information regarding the interface, you might see concatenated results.

Information About Implementing SNMP

To implement SNMP, you need to understand the concepts described in this section.

SNMP Functional Overview

The SNMP framework consists of three parts:

- SNMP manager
- SNMP agent
- Management Information Base (MIB)

SNMP Manager

The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a *network management system* (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on such a device. A variety of network management applications are available for use with SNMP.

SNMP Agent

The SNMP agent is the software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The agent and MIB reside on the router. To enable the SNMP agent, you must define the relationship between the manager and the agent.

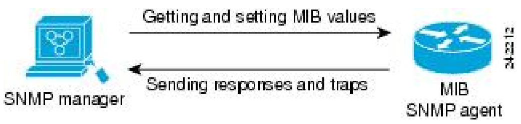
MIB

The *Management Information Base* (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects. Within the MIB there are collections of related objects, defined in MIB modules. MIB modules are written in the SNMP MIB module language, as defined in STD 58, RFC 2578, RFC 2579, and RFC 2580. Note that individual MIB modules are also referred to as MIBs; for example, the Interfaces Group MIB (IF-MIB) is a MIB module within the MIB on your system.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change through Get or Set operations. A manager can get a value from an agent or store a value into that agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to manager requests to get or set data.

The figure below, illustrates the communications relationship between the SNMP manager and agent. A manager can send the agent requests to get and set MIB values. The agent can respond to these requests. Independent of this interaction, the agent can send unsolicited notifications (traps) to the manager to notify the manager of network conditions.

Figure 5: Communication Between an SNMP Agent and Manager



SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. On Cisco IOS XR software, unsolicited (asynchronous) notifications can be generated only as *traps*. Traps are messages alerting the SNMP manager to a condition on the network. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Note Inform requests (inform operations) are not supported in Cisco IOS XR software.

Traps are less reliable than informs because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, traps are often preferred because informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, and an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources.

Figure 6: Trap Received by the SNMP Manager

In this illustration, the agent router sends a trap to the SNMP manager. Although the manager receives the trap, it does not send any acknowledgment to the agent. The agent has no way of knowing that the trap reached its destination.

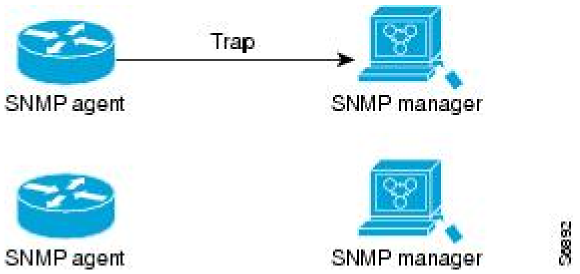
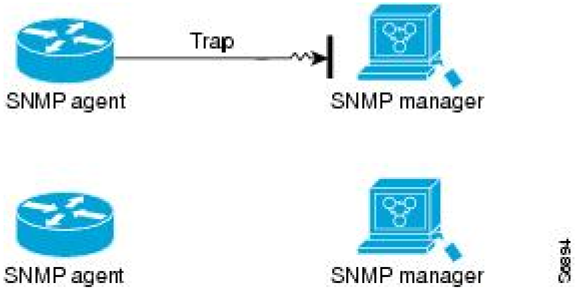


Figure 7: Trap Not Received by the SNMP Manager

In this illustration, the agent sends a trap to the manager, but the trap does not reach the manager. Because the agent has no way of knowing that the trap did not reach its destination, the trap is not sent again. The manager never receives the trap.



SNMP Versions

Cisco IOS XR software supports the following versions of SNMP:

- Simple Network Management Protocol Version 1 (SNMPv1)
- Simple Network Management Protocol Version 2c (SNMPv2c)
- Simple Network Management Protocol Version 3 (SNMPv3)

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is defined by an IP address access control list and password.

SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: no such object exceptions, no such instance exceptions, and end of MIB view exceptions.

SNMPv3 is a security model. A *security model* is an authentication strategy that is set up for a user and the group in which the user resides. A *security level* is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when an SNMP packet is handled. See Security Models and Levels for SNMPv1, v2, v3, on page 295 for a list of security levels available in SNMPv3. The SNMPv3 feature supports RFCs 3411 to 3418.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS-XR software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Comparison of SNMPv1, v2c, and v3

SNMP v1, v2c, and v3 all support the following operations:

- get-request—Retrieves a value from a specific variable.
- get-next-request—Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
- get-response—Operation that replies to a get-request, get-next-request, and set-request sent by an NMS.
- set-request—Operation that stores a value in a specific variable.
- trap—Unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

Table 25: SNMPv1, v2c, and v3 Feature Support

Feature	SNMP v1	SNMP v2c	SNMP v3
Get-Bulk Operation	No	Yes	Yes
Inform Operation	No	Yes (No on the Cisco IOS XR software)	Yes (No on the Cisco IOS XR software)
64 Bit Counter	No	Yes	Yes
Textual Conventions	No	Yes	Yes
Authentication	No	No	Yes
Privacy (Encryption)	No	No	Yes

Feature	SNMP v1	SNMP v2c	SNMP v3
Authorization and Access Controls (Views)	No	No	Yes

Security Models and Levels for SNMPv1, v2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

Table 26: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the HMAC[1]-MD5[2] algorithm or the HMAC-SHA[3].
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES[4] 56-bit encryption in addition to authentication based on the CBC[5] DES (DES-56) standard.
v3	authPriv	HMAC-MD5 or HMAC-SHA	3DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 168-bit 3DES[6] level of encryption.
v3	authPriv	HMAC-MD5 or HMAC-SHA	AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 128-bit AES[7] level of encryption.

[1] Hash-Based Message Authentication Code
[2] Message Digest 5
[3] Secure Hash Algorithm
[4] Data Encryption Standard
[5] Cipher Block Chaining
[6] Triple Data Encryption Standard

[7] Advanced Encryption Standard

SNMPv3 Benefits

SNMPv3 provides secure access to devices by providing authentication, encryption and access control. These added security benefits secure SNMP against the following security threats:

- Masquerade—The threat that an SNMP user may assume the identity of another SNMP user to perform management operations for which that SNMP user does not have authorization.
- Message stream modification—The threat that messages may be maliciously reordered, delayed, or replayed (to an extent that is greater than can occur through the natural operation of a subnetwork service) to cause SNMP to perform unauthorized management operations.
- Disclosure—The threat that exchanges between SNMP engines could be eavesdropped. Protecting against this threat may be required as a matter of local policy.

In addition, SNMPv3 provides access control over protocol operations on SNMP managed objects.

SNMPv3 Costs

SNMPv3 authentication and encryption contribute to a slight increase in the response time when SNMP operations on MIB objects are performed. This cost is far outweighed by the security advantages provided by SNMPv3.

Table 27: Order of Response Times from Least to Greatest

Security Model	Security Level
SNMPv2c	noAuthNoPriv
SNMPv3	noAuthNoPriv
SNMPv3	authNoPriv
SNMPv3	authPriv

User-Based Security Model

SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

USM uses two authentication protocols:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

USM uses Cipher Block Chaining (CBC)-DES (DES-56) as the privacy protocol for message encryption.

View-Based Access Control Model

The View-Based Access Control Model (VACM) enables SNMP users to control access to SNMP managed objects by supplying read, write, or notify access to SNMP objects. It prevents access to objects restricted by views. These access policies can be set when user groups are configured with the **snmp-server group** command.

MIB Views

For security reasons, it is often valuable to be able to restrict the access rights of some groups to only a subset of the management information within the management domain. To provide this capability, access to a management object is controlled through MIB views, which contain the set of managed object types (and, optionally, the specific instances of object types) that can be viewed.

Access Policy

Access policy determines the access rights of a group. The three types of access rights are as follows:

- read-view access—The set of object instances authorized for the group when objects are read.
- write-view access—The set of object instances authorized for the group when objects are written.
- notify-view access—The set of object instances authorized for the group when objects are sent in a notification.

IP Precedence and DSCP Support for SNMP

SNMP IP Precedence and differentiated services code point (DSCP) support delivers QoS specifically for SNMP traffic. You can change the priority setting so that SNMP traffic generated in a router is assigned a specific QoS class. The IP Precedence or IP DSCP code point value is used to determine how packets are handled in weighted random early detection (WRED).

After the IP Precedence or DSCP is set for the SNMP traffic generated in a router, different QoS classes cannot be assigned to different types of SNMP traffic in that router.

The IP Precedence value is the first three bits in the type of service (ToS) byte of an IP header. The IP DSCP code point value is the first six bits of the differentiate services (DiffServ Field) byte. You can configure up to eight different IP Precedence markings or 64 different IP DSCP markings.

How to Implement SNMP on Cisco IOS XR Software

This section describes how to implement SNMP.

The **snmp-server** commands enable SNMP on Management Ethernet interfaces by default.

Configuring SNMPv3

This task explains how to configure SNMPv3 for network management and monitoring.

Note No specific command enables SNMPv3; the first **snmp-server** global configuration command (config), that you issue enables SNMPv3. Therefore, the sequence in which you issue the **snmp-server** commands for this task does not matter.

Procedure

Step 1 **configure**

Step 2 **snmp-server view** *view-name oid-tree* {**included** | **excluded**}

Example:

```
RP/0/RP0:hostname(config)# snmp-server view
view_name 1.3.6.1.2.1.1.5 included
```

Creates or modifies a view record.

Step 3 **snmp-server group** *name* {**v1** | **v2c** | **v3** {**ipv4** | **ipv6** | **context**}} [**read** *view*] [**write** *view*] [**notify** *view*] [*access-list-name*]

Example:

```
RP/0/RP0:hostname(config)# snmp-server group
group_name v3 noauth read view_name1 write view_name2
```

Configures a new SNMP group or a table that maps SNMP users to SNMP views.

Step 4 **snmp-server user** *username groupname* {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} {**clear** | **encrypted**} *auth-password* [**priv des56** {**clear** | **encrypted**} *priv-password*]]} [*access-list-name*] [**sdrowner**] [**systemowner**]

Example:

```
RP/0/RP0:hostname(config)# snmp-server user
noauthuser group_name v3
```

Configures a new user to an SNMP group.

Step 5 **commit**

Configuring SNMP Trap Notifications

This task explains how to configure the router to send SNMP trap notifications.

Procedure

Step 1 **configure**

Step 2 **snmp-server group** *name*{ **v1** | **v2** | **v3** } { **ipv4** | **ipv6** | **context** } [**read** *view*] [**write** *view*] [**notify** *view*] [*access-list-name*]

Example:

```
RP/0/RP0:hostname(config)# snmp-server group g1 v3 ipv4
view_name 1.3.6.1.2.1.1.5 included
```

Configures a new SNMP group or a table that maps SNMP users to SNMP views.

Step 3 **snmp-server user** *username groupname* {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} {**clear** | **encrypted**} *auth-password* [**priv des56** {**clear** | **encrypted**} *priv-password*]]} [*access-list-name*] [**sdrowner**] [**systemowner**]

Example:

```
RP/0/RP0:hostname(config)# snmp-server user
noauthuser group_name v3
```

Configures a new user to an SNMP group.

Step 4 **snmp-server host** *address* [**traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

Example:

```
RP/0/RP0:hostname(config)# snmp-server host 12.26.25.61 traps version 3
noauth userV3noauth
```

Specifies SNMP trap notifications, the version of SNMP to use, the security level of the notifications, and the recipient (host) of the notifications.

Step 5 **snmp-server traps** [*notification-type*]

Example:

```
RP/0/RP0:hostname(config)# snmp-server traps bgp
```

Enables the sending of trap notifications and specifies the type of trap notifications to be sent.

- If a trap is not specified with the *notification-type* argument, all supported trap notifications are enabled on the router. To display which trap notifications are available on your router, enter the **snmp-server traps ?** command.

Step 6 **commit**

Step 7 (Optional) **show snmp host**

Example:

```
RP/0/RP0:hostname# show snmp host
```

Displays information about the configured SNMP notification recipient (host), port number, and security model.

Configure SNMP on a Node

This procedure enables the user to configure SNMP on a node ; the node now performs as an SNMP agent.

Procedure

Step 1 **configure**

Step 2 **snmp-server community public** *community-string* [**RO** | **RW**] [**SDROwner** | **SystemOwner**]

Example:

```
RP/0/RP0:hostname(config) # snmp-server community c1 RW SystemOwner
```

Configures the community access string to permit access to the Simple Network Management Protocol (SNMP). The **RW** keyword specifies read-write access and the authorized management stations can both, retrieve and modify MIB objects.

Step 3 **snmp-server traps otn**

Example:

```
RP/0/RP0:hostname(config) # snmp-server traps otn
```

Enables SNMP OTN traps.

Step 4 **snmp-server host** *host-address* **traps version**[**1** | **2c** | **3**] **public udp-port** *udp-port number*

Example:

```
RP/0/RP0:hostname(config) # snmp-server host 10.1.1.1 traps version 2c public udp-port 100
```

Configures the host address, SNMP version and the udp port number to which the notifications need to be sent.

Step 5 **commit**

Setting the Contact, Location, and Serial Number of the SNMP Agent

This task explains how to set the system contact string, system location string, and system serial number of the SNMP agent.

Note The sequence in which you issue the **snmp-server** commands for this task does not matter.

Procedure

Step 1 **configure**

Step 2 (Optional) **snmp-server contact** *system-contact-string*

Example:

```
RP/0/RP0:hostname(config)# snmp-server contact
Dial System Operator at beeper # 27345
```

Sets the system contact string.

Step 3 (Optional) **snmp-server location** *system-location*

Example:

```
RP/0/RP0:hostname(config)# snmp-server location
Building 3/Room 214
```

Sets the system location string.

Step 4 (Optional) **snmp-server chassis-id** *serial-number*

Example:

```
RP/0/RP0:hostname(config)# snmp-server chassis-id 1234456
```

Sets the system serial number.

Step 5 **commit**

Defining the Maximum SNMP Agent Packet Size

This task shows how to configure the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

Note The sequence in which you issue the **snmp-server** commands for this task does not matter.

Procedure

Step 1 **configure**

Step 2 (Optional) **snmp-server packetsize** *byte-count*

Example:

```
RP/0/RP0:hostname(config)# snmp-server packetsize 1024
```

Sets the maximum packet size.

Step 3 **commit**

Changing Notification Operation Values

After SNMP notifications have been enabled, you can specify a value other than the default for the source interface, message queue length, or retransmission interval.

This task explains how to specify a source interface for trap notifications, the message queue length for each host, and the retransmission interval.

Note The sequence in which you issue the **snmp-server** commands for this task does not matter.

Procedure

Step 1 **configure**

Step 2 (Optional) **snmp-server trap-source** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# snmp-server trap-source POS 0/0/1/0
```

Specifies a source interface for trap notifications.

Step 3 (Optional) **snmp-server queue-length** *length*

Example:

```
RP/0/RP0:hostname(config)# snmp-server queue-length 20
```

Establishes the message queue length for each notification.

Step 4 (Optional) **snmp-server trap-timeout** *seconds*

Example:

```
RP/0/RP0:hostname(config)# snmp-server trap-timeout 20
```

Defines how often to resend notifications on the retransmission queue.

Step 5 **commit**

Setting IP Precedence and DSCP Values

This task describes how to configure IP Precedence or IP DSCP for SNMP traffic.

Before you begin

SNMP must be configured.

Procedure

Step 1 **configure**

Step 2 Use one of the following commands:

- **snmp-server ipv4 precedence** [*value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**]
- **snmp-server ipv4 dscp** [*value* | **af11...13** | **af21...23** | **af31...33** | **af41...43** | **cs1...cs7** | **default** | **ef**]

Example:

```
RP/0/RP0:hostname(config)# snmp-server dscp 24
```

Configures an IP precedence or IP DSCP value for SNMP traffic.

Step 3 **commit**

Displaying SNMP Context Mapping

The SNMP agent serves queries based on SNMP contexts created by the client features. There is a context mapping table. Each entry in the context mapping table includes a context name, the name of the feature that created the context, and the name of the specific instance of the feature.

Procedure

show snmp context-mapping

Example:

```
RP/0/RP0:hostname# show snmp context-mapping
```

Displays the SNMP context mapping table.

Monitoring Packet Loss

It is possible to monitor packet loss by configuring the generation of SNMP traps when packet loss exceeds a specified threshold. The configuration described in this task enables the creation of entries in the MIB tables of the EVENT-MIB. This can then be monitored for packet loss using SNMP GET operations.

Before you begin

Note Entries created in the EVENT-MIB MIB tables using the configuration described in this task cannot be altered using an SNMP SET.

Entries to the EVENT-MIB MIB tables created using an SNMP SET cannot be altered using the configuration described in this task.

Procedure

snmp-server mibs eventmib packet-loss *type interface-path-id* **falling** *lower-threshold* **interval** *sampling-interval* **rising** *upper-threshold*

Example:

```
RP/0/RP0:hostname(config)# snmp-server mibs eventmib packet-loss TenGigE 0/2/0/3 falling 1
 interval 5 rising 2
```

Generates SNMP EVENT-MIB traps for the interface when the packet loss exceeds the specified thresholds. Up to 100 interfaces can be monitored.

falling *lower-threshold* —Specifies the lower threshold. When packet loss between two intervals falls below this threshold and an mteTriggerRising trap was generated previously, a SNMP mteTriggerFalling trap is generated. This trap is not generated until the packet loss exceeds the upper threshold and then falls back below the lower threshold.

interval *sampling-interval* —Specifies how often packet loss statistics are polled. This is a value between 5 and 1440 minutes, in multiples of 5.

rising *upper-threshold* —Specifies the upper threshold. When packet loss between two intervals increases above this threshold, an SNMP mteTriggreRising trap is generated. This trap is not generated until the packet loss drops below the lower threshold and then rises above the upper threshold.

Configuring MIB Data to be Persistent

Many SNMP MIB definitions define arbitrary 32-bit indices for their object tables. MIB implementations often do a mapping from the MIB indices to some internal data structure that is keyed by some other set of data. In these MIB tables the data contained in the table are often other identifiers of the element being modelled. For example, in the ENTITY-MIB, entries in the entPhysicalTable are indexed by the 31-bit value, entPhysicalIndex, but the entities could also be identified by the entPhysicalName or a combination of the other objects in the table.

Because of the size of some MIB tables, significant processing is required to discover all the mappings from the 32-bit MIB indices to the other data which the network management station identifies the entry. For this reason, it may be necessary for some MIB indices to be persistent across process restarts, switchovers, or device reloads. The ENTITY-MIB entPhysicalTable and CISCO-CLASS-BASED-QOS-MIB are two such MIBs that often require index values to be persistent.

Also, because of query response times and CPU utilization during CISCO-CLASS-BASED-QOS-MIB statistics queries, it is desirable to cache service policy statistics.

Procedure

Step 1 (Optional) **snmp-server mibs cbqosmib persist**

Example:

```
RP/0/RP0:hostname(config)# snmp-server mibs cbqosmib persist
```

Enables persistent storage of the CISCO-CLASS-BASED-QOS-MIB data.

Step 2 (Optional) **snmp-server mibs cbqosmib cache refresh time** *time*

Example:

```
RP/0/RP0:hostname(config)# snmp-server mibs cbqosmib cache
refresh time 45
```

Enables QoS MIB caching with a specified cache refresh time.

Step 3 (Optional) **snmp-server mibs cbqosmib cache service-policy count** *count*

Example:

```
RP/0/RP0:hostname(config)# snmp-server mibs cbqosmib cache
service-policy count 50
```

Enables QoS MIB caching with a limited number of service policies to cache.

Step 4 (Optional) **snmp-server ifindex persist**

Example:

```
RP/0/RP0:hostname(config)# snmp-server ifindex persist
```

Enables ifIndex persistence on all interfaces that have entries in the ifIndex table of the IF-MIB. When enabled, this command retains the mapping between the ifName object values and the ifIndex object values persistent during reloads, allowing for consistent identification of specific interfaces using SNMP.

Configuring LinkUp and LinkDown Traps for a Subset of Interfaces

By specifying a regular expression to represent the interfaces for which you are interested in setting traps, you can enable or disable linkUp and linkDown traps for a large number of interfaces simultaneously.

Before you begin

SNMP must be configured.

Procedure

Step 1 **configure**

Step 2 **snmp-server interface subset** *subset-number* **regular-expression** *expression*

Example:

```
RP/0/RP0:hostname(config)# snmp-server interface subset 10
    regular-expression "^Gig[a-zA-Z]+[0-9/]+\."
RP/0/RP0:hostname(config-snmp-if-subset)#
```

Enters snmp-server interface mode for the interfaces identified by the regular expression.

The subset-number argument identifies the set of interfaces, and also assigns a priority to the subset in the event that an interface is included in more than one subset. Lower numbers have higher priority and their configuration takes precedent over interface subsets with higher numbers.

The *expression* argument must be entered surrounded by double quotes.

Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in for more information regarding regular expressions.

Step 3 **notification linkupdown disable**

Example:

```
RP/0/RP0:hostname(config-snmp-if-subset)# notification linkupdown disable
```

Disables linkUp and linkDown traps for all interfaces being configured. To enable previously disabled interfaces, use the **no** form of this command.

Step 4 **commit**

Step 5 (Optional) **show snmp interface notification subset** *subset-number*

Example:

```
RP/0/RP0:hostname# show snmp interface notification subset 10
```

Displays the linkUp and linkDown notification status for all interfaces identified by the subset priority.

Step 6 (Optional) **show snmp interface notification regular-expression** *expression*

Example:

```
RP/0/RP0:hostname# show snmp interface notification
    regular-expression "^Gig[a-zA-Z]+[0-9/]+\."
```

Displays the linkUp and linkDown notification status for all interfaces identified by the regular expression.

Step 7 (Optional) **show snmp interface notification** *type interface-path-id*

Example:

```
RP/0/RP0:hostname# show snmp interface notification
    tengige 0/4/0/3.10
```

Displays the linkUp and linkDown notification status for the specified interface.

Generic IETF Traps

OTN supports the generic IETF traps listed in the following table.

call information	(Optional) Controls SNMP ISDN call information notifications, as defined in the CISCO-ISDN-MIB (enterprise 1.3.6.1.4.1.9.9.26.2). Notification types are: • demandNbrCallInformation (1) This notification is sent to the manager whenever a successful call clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type. • demandNbrCallDetails (2) This notification is sent to the manager whenever a call connects, or clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type.
chan-not-avail	(Optional) Controls SNMP ISDN channel-not-available notifications. ISDN PRI channel-not-available traps are generated when a requested DS-0 channel is not available, or when there is no modem available to take the incoming call. These notifications are available only for ISDN PRI interfaces.
ietf	(Optional) Controls the SNMP ISDN IETF traps.
isdnu-interface	(Optional) Controls SNMP ISDN U interface notifications.
layer2	(Optional) Controls SNMP ISDN Layer 2 transition notifications.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ISDN notifications are defined in the CISCO-ISDN-MIB.my and CISCO-ISDNU-IF-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Availability of notifications will depend on your platform. To see what notifications are available, use the **snmp-server enable traps isdn ?** command.

If you do not enter an **snmp-server enable traps isdn** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one

snmp-server enable traps isdn command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one snmp-server host command

Examples of IETF Traps

The following example shows how to determine what notification types are available on a Cisco AS5300 and then shows how to enable channel-not-available and Layer 2 informs:

```
NAS(config)# snmp-server enable traps isdn ?
call-information  Enable SNMP isdn call information traps
 chan-not-avail    Enable SNMP isdn channel not avail traps
ietf              Enable SNMP isdn ietf traps
 layer2            Enable SNMP isdn layer2 transition traps
<cr>
NAS(config)# snmp-server enable traps isdn chan-not-avail layer2
NAS(config)# snmp-server host myhost.cisco.com informs version 2c public isdn
```

SNMP Traps Supported in OTN

The following table lists the SNMP Traps Supported in OTN.

Table 28: SNMP Traps Supported in OTN

MIB Module
coiOtnIfOTUStatus
coiOtnIfODUStatus

MIB Supported in OTN

The following table lists the MIBs supported in OTN.

Table 29: MIBs Supported in OTN

MIB Module
RADIUS-AUTH-CLIENT-MIB
RADIUS-ACC-CLIENT-MIB
RADIUS-AUTH-CLIENT-MIB
CISCO-FLOW-MONITOR-MIB
CISCO-IP-CBR-METRICS-MIB
CISCO-FLOW-CLONE-MIB
ATM-MIB

MIB Module
ATM2-MIB
CISCO-ATM-EXT-MIB
IMA-MIB
CISCO-ATM-QOS-MIB
CISCO-OAM-MIB
IEEE8023-LAG-MIB
CISCO-CDP-MIB
ISIS-MIB
CISCO-CONFIG-MAN-MIB
CISCO-IPSEC-POLICY-MAP-MIB
CISCO-IPSEC-MIB
CISCO-IPSEC-FLOW-MONITOR-MIB
ETHERLIKE-MIB
CISCO-OTN-IF-MIB
CISCO-FLASH-MIB
FRAME-RELAY-DTE-MIB
CISCO-FRAME-RELAY-MIB
MFR-MIB
CISCO-CONFIG-COPY-MIB
CISCO-LICENSE-MGMT-MIB
CISCO-ENTITY-REDUNDANCY-MIB
CISCO-ENHANCED-MEMPOOL-MIB
CISCO-MEMORY-POOL-MIB
CISCO-PROCESS-MIB
CISCO-SYSLOG-MIB
CISCO-SYSTEM-MIB
CISCO-SELECTIVE-VRF-DOWNLOAD-MIB
CISCO-IETF-BFD-MIB
CISCO-NTP-MIB
IPv6-FORWARD-MIB
IP-FORWARD-MIB
RSVP-MIB

MIB Module
CISCO-TCP-MIB
TCP-MIB
UDP-MIB
BGP4-MIB
CISCO-BGP4-MIB
CISCO-HSRP-MIB
CISCO-HSRP-EXT-MIB
RFC2011-MIB
CISCO-MLD-SNOOPING-MIB
OSPF-TRAP-MIB
OSPF-MIB
CISCO-IETF-VRRP-07-MIB
VRRP-MIB
OSPFV3-MIB
CISCO-IP-STAT-MIB
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
LLDP-MIB
IEEE8021-CFM-MIB
OAM-MIB
CISCO-IETF-VPLS-BGP-EXT-MIB
CISCO-IETF-PW-FR-MIB
CISCO-IETF-PW-MIB
CISCO-IETF-PW-MPLS-MIB
CISCO-IETF-PW-ENET-MIB
CISCO-IETF-VPLS-LDP-MIB
CISCO-IETF-VPLS-GENERIC-MIB
CISCO-TAP2-MIB
CISCO-USER-CONNECTION-TAP-MIB
CISCO-IP-TAP-MIB
CISCO-RTTMON-MIB
MPLS-LDP-STD-MIB
MPLS-LDP-GENERIC-STD-MIB

MIB Module
MPLS-LSR-STD-MIB
CISCO-MPLS-TE-STD-EXT-MIB
MPLS-TE-STD-MIB
CISCO-MPLS-TE-STD-EXT-MIB
CISCO-IETF-FRR-MIB
CISCO-IETF-MPLS-TE-P2MP-STD-MIB
MPLS-L3VPN-STD-MIB
DS1-MIB
CISCO-DS3-MIB
DS3-MIB
CISCO-FABRIC-C12K-MIB
CISCO-FABRIC-MCAST-APPL-MIB
CISCO-FABRIC-MCAST-MIB
CISCO-FABRIC-HFR-MIB
CISCO-CLASS-BASED-QOS-MIB
CISCO-CLASS-BASED-QOS-MIB
CISCO-TEST-MIB
CISCO-MIBD-ROUTE-TEST-MIB
CISCO-MIBD-INT-TEST-MIB
CISCO-ENTITY-ASSET-MIB
BRIDGE-MIB
CISCO-BULK-FILE-MIB
CISCO-BGP-POLICY-ACCOUNTING-MIB
CISCO-CONTEXT-MAPPING-MIB
CISCO-ENHANCED-IMAGE-MIB
ENTITY-MIB
ENTITY-STATE-MIB
CISCO-ENTITY-STATE-EXT-MIB
EVENT-MIB
DISMAN-EXPRESSION-MIB
CISCO-ENTITY-FRU-CONTROL-MIB
CISCO-FTP-CLIENT-MIB

MIB Module
IF-MIB
CISCO-IF-EXTENSION-MIB
IETF-TCP-MIB
RFC2465-MIB
IPV6-MIB
IETF-UDP-MIB
MAU-MIB
CISCO-MAU-EXT-MIB
CISCO-IETF-MSDP-MIB
CISCO-IETF-PIM-EXT-MIB
PIM-MIB
CISCO-PIM-MIB
CISCO-IETF-IPMROUTE-MIB
MGMDSTDMIB-MIB
IPV6-MLD-MIB
NOTIFICATION-LOG-MIB
CISCO-P2P-IF-MIB
CISCO-PING-MIB
CISCO-RF-MIB
CISCO-ENTITY-SENSOR-MIB
APS-MIB
CISCO-SONET-MIB
SONET-MIB
ATM-FORUM-MIB
ATM-FORUM-ADDR-REG
ATM-FORUM-SRVC-REG
CISCO-SC-MIB
HCNUM-TC
CISCO-CLASS-BASED-QOS-MIB
CISCO-SESS-BORDER-CTRLR-EVENT-MIB
CISCO-SESS-BORDER-CTRLR-CALL-STATS-MIB
mgmtrap

MIB Module
dbltrap
SNMPv2-MIB

CHAPTER 29

Configure Performance Monitoring

This chapter describes the Cisco IOS XR commands to configure the performance monitoring for various controllers.

Display the PM Parameters of a Controller

Perform this task to view the PM parameters of a controller. Before viewing the PM parameters, a controller should be created.

Procedure

show controllers *name-of-the-controller R/S/I/P* **pm [current | history] [15-min | 24-hour] layer name {optics | ocn | ether | otn and gfp | otn and fec | otn and pathmonitor | otn and tcm}** *bucket number* **1-32**

Example:

```
RP/0/RP0:hostname # show controllers optics 0/0/0/2 pm current 15-min optics 12
RP/0/RP0:hostname # show controllers optics 0/0/0/2 pm current 24-hour optics 5
RP/0/RP0:hostname # show controllers optics 0/0/0/2 pm history 15-min optics1 1
RP/0/RP0:hostname # show controllers optics 0/0/0/2 pm history 24-hour optics 5
```

Displays the performance parameter of current values tab for 15-minutes and 24-hour intervals.

Clears the PM Parameters of a Controller

Perform this task to clear the PM parameters of a controller. Before clearing the PM parameters, a controller should be created.

Procedure

clear controllers *name-of-the-controller R/S/I/P* **pm [15-min | 24-hour] clear**

Example:

```
RP/0/RP0:hostname # clear controllers OTU1E 0/4/0/0 pm 15-min clear
RP/0/RP0:hostname # clear controllers optics 0/4/0/0 pm 24-hour clear
```

clears the performance parameter of current values tab for 15-minutes and 24-hour intervals.

Configure the Time Interval for Optics Performance Monitoring (PM) Threshold

Perform this task to configure the time interval for Optics PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller optics** *R/S/I/P*

Example:

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

Enters the Optics controller configuration mode.

Step 3 **pm [15-min | 24-hour] optics [report | threshold]** *{lbc | opr | opt} [max-tca | min-tca]* **enable**

Example:

```
RP/0/RP0:hostname (config-optics)# pm 15-min optics report lbc max-tca enable
```

Specifies the PM interval for the optics controller and set report value for the layer.

Step 4 **pm [15-min | 24-hour] optics [report | threshold]** *{lbc | opr | opt} [max | min] value*

Example:

```
RP/0/RP0:hostname (config-optics)# pm 15-min optics threshold opr max 15
```

Specifies the PM interval for the optics controller and set threshold value for the opr max. The value of opr max threshold ranges from 1 to 4294967295.

Step 5 **commit**

Configure the Time Interval for Optical Carrier (OC) Performance Monitoring (PM) Threshold

Perform this task to configure the time interval for Optical Carrier (OC) PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller [oc48 | oc192]***R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller oc48 0/0/0/5
```

Enters the oc48 controller configuration mode.

Step 3 **pm [15-min | 24-hour] ocn [report | threshold]** *parameter name* **disable**

Example:

```
RP/0/RP0:hostname (config-oc48)# pm 15-min ocn report cv-l-fe disable
```

Specifies the PM interval for the oc controller and set report value for the layer.

Step 4 **pm [15-min | 24-hour] ocn [report | threshold]** *parameter name value*

Example:

```
RP/0/RP0:hostname (config-oc48)# pm 15-min ocn threshold cv-l-ne 8
```

Specifies the PM interval for the oc controller and set threshold value for the layer. The value of cv-l-ne layer ranges from 0 to 849657600.

Step 5 **commit**

Configure the Time Interval for Synchronous Transport Signal (STS) PM Threshold

Perform this task to configure the time interval for Synchronous Transport Signal (STS) PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller sts48c** *R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller sts48c 0/0/0/4
```

Enters the sts48c controller configuration mode.

Step 3 **pm [15-min | 24-hour] sts [report | threshold]** *{cv-p | es-p | ses-p | uas-p}* **disable**

Example:

```
RP/0/RP0:hostname (config-sts48c)# pm 15-min sts report es-p disable
```

Specifies the PM interval for the sts controller and set report value for the layer.

Step 4 **pm [15-min | 24-hour] sts [report | threshold]** *{cv-p | es-p | ses-p | uas-p} value*

Example:

```
RP/0/RP0:hostname (config-sts48c)# pm 15-min sts threshold ses-p 8
```

Specifies the PM interval for the oc controller and set threshold value for the layer. The value of ses-p ranges from 0 to 86400.

Step 5 **commit**

Configure the Time Interval for Synchronous Transport Module (STM) PM Threshold

Perform this task to configure the time interval for Synchronous Transport Module (STM) PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller {stm1 | stm4 | stm16 | stm64 | stm256}***R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller stm4 0/0/0/5
```

Enters the stm4 controller configuration mode.

Step 3 **pm [15-min | 24-hour] stm [report | threshold]** *parameter name* **disable**

Example:

```
RP/0/RP0:hostname (config-stm4)# pm 15-min stm report eb-l-fe disable
```

Specifies the PM interval for the stm controller and set report value for the layer.

Step 4 **pm [15-min | 24-hour] stm [report | threshold]** *parameter name value*

Example:

```
RP/0/RP0:hostname (config-stm4)# pm 24-hour stm threshold ses-l-fe 8
```

Specifies the PM interval for the stm controller and set threshold value for the layer. The ses-l-fe threshold value ranges from 0 to 86400.

Step 5 **commit**

Configure the Time Interval for Virtual Concatenation (VC) Performance Monitoring (PM) Threshold

Perform this task to configure the time interval for Virtual Concatenation (VC) PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller** *name-of-the-controller R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller vc4-16c 0/2/0/0
```

Enters the vc4-16c controller configuration mode.

Step 3 **pm [15-min | 24-hour] ho-vc [report | threshold]** *parameter name* **disable**

Example:

```
RP/0/RP0:hostname (config-vc4-16c)# pm 15-min ho-vc report bbe-p disable
```

Specifies the PM interval for the vc controller and set report value for the layer.

Step 4 **pm [15-min | 24-hour] ho-vc [report | threshold]** *parameter name* **disable**

Example:

```
RP/0/RP0:hostname (config-vc4-16c)# pm 24-hour ho-vc threshold ses-p 22
```

Specifies the PM interval for the vc controller and set report value for the layer. The value of ses-p threshold ranges from 0 to 86400.

Step 5 **commit**

Configure the Time Interval for ODU Performance Monitoring (PM) Threshold

Perform this task to configure the time interval for ODU PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller odu** *[HO | LO] R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller odu2 0/0/0/2
```

Enters the ODU2 controller configuration mode.

Step 3 **tcm id** *value* **perf-mon** *[Enable | Disable]*

Example:

```
RP/0/RP0:hostname (config-odu2) # tcm id 1 perf-mon enable
```

Enables the performance monitoring.

Step 4 **pm [15-min | 24-hour] [gfp | otn] [report | threshold]** *{rx-bit-err | rx-crc-err | rx-csf-stats | rx-inv-type | rx-lfd-stats}* **enable**

Example:

```
RP/0/RP0:hostname (config-odu2)# pm 15-min gfp report rx-crc-err enable
```

Specifies the PM interval for the odu controller and set report value for the gfp layer.

Step 5 **pm [15-min | 24-hour] [gfp | otn pathmonitor | otn tcm] [report | threshold]** *{rx-bit-err | rx-crc-err | rx-csf-stats | rx-inv-type |rx-lfd-stats}* **enable**

Example:

```
RP/0/RP0:hostname (config-odu2)# pm 15-min otn pathmonitor threshold uas-fe 8
```

Specifies the PM interval for the odu controller and set threshold value for the otn layer. Threshold value for uas-fe ranges from 0 to 900.

Step 6 **commit**

Configure the Time Interval for Ethernet Performance Monitoring (PM) Threshold

Perform this task to configure the time interval for ethernet PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller ethernet** *R/S/I/P*

Example:

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

Enters the ethernet controller configuration mode.

Step 3 **pm {15-min | 24-hour} ether {report | threshold}** *value*

Example:

```
RP/0/RP0:hostname (config-tenGigECtrlr)# pm 24-hour ether report in-Mcast enable
RP/0/RP0:hostname (config-tenGigECtrlr)# pm 15-min ether threshold in-Bcast enable
```

Specifies the PM interval for the ethernet controller and set threshold value for the layer.

Step 4 **commit**

Configure the Time Interval for OTU Performance Monitoring (PM) Threshold

Perform this task to configure the time interval for OTU PM threshold.

Procedure

Step 1 **configure**

Step 2 **controller otu** *[HO | LO] R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller otu1 0/0/0/1
```

Enters the OTU1 controller configuration mode. Performance monitoring is enabled by-default for otu controllers.

Step 3 **pm [15-min | 24-hour] [fec | otn] [report | threshold]** *[ec-bits | uc-words]* **disable**

Example:

```
RP/0/RP0:hostname (config-otu1)# pm 15-min fec report ec-bits disable
```

Specifies the PM interval for the otu controller and set report value for the fec layer.

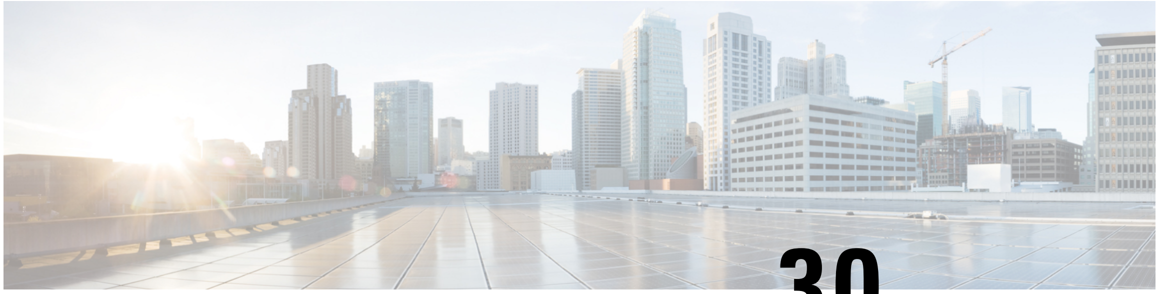
Step 4 **pm [15-min | 24-hour] [fec | otn] [report | threshold]** *threshold type value*

Example:

```
RP/0/RP0:hostname (config-otu1)# pm 15-min otn threshold bber-ne 55
```

Specifies the PM interval for the otu controller and set report value for the otn layer. Threshold value for bber-ne ranges from 0 to 100000.

Step 5 **commit**



CHAPTER 30

Configure Fault Management

This chapter describes the procedures to create and load the alarm profiles.

Create a Fault Profile

Perform this task to create a fault profile.

Procedure

Step 1 **configure**

Step 2 **fault-profile** *name*

Example:

```
RP/0/RP0:hostname (config)# fault-profile test
```

Creates a fault profile.

Step 3 **fault-identifier subsystem** *type-of-the-subsystem* **fault-type** *type-of-the-fault* **fault-tag** *type-of-the-tag* **sas** *severity-of-the-alarm* **nsas** *severity-of-the-alarm*

Example:

```
RP/0/RP0:hostname (config-fault-profile)# fault-identifier subsystem XR
    fault-type HW_ETHERNET fault-tag ETHER_SIGLOSS sas CRITICAL nsas MAJOR
```

Configures the fault profile.

Step 4 **fault-profile** *name-of-the-fault-profile* **description** *description-of-the-fault-profile*

Example:

```
RP/0/RP0:hostname (config-fault-profile)# fault-profile test description this is test profile
```

Defines description of the profile.

Step 5 **commit**

Load a Fault Profile

Before you begin

Create a fault profile. See Create a Fault Profile, on page 323.

Procedure

Step 1 **configure**

Step 2 **fault-profile** *name-of-the-fault-profile*

Example:

```
RP/0/RP0:hostname (config)# fault-profile test
```

Enter the fault profile configuration mode.

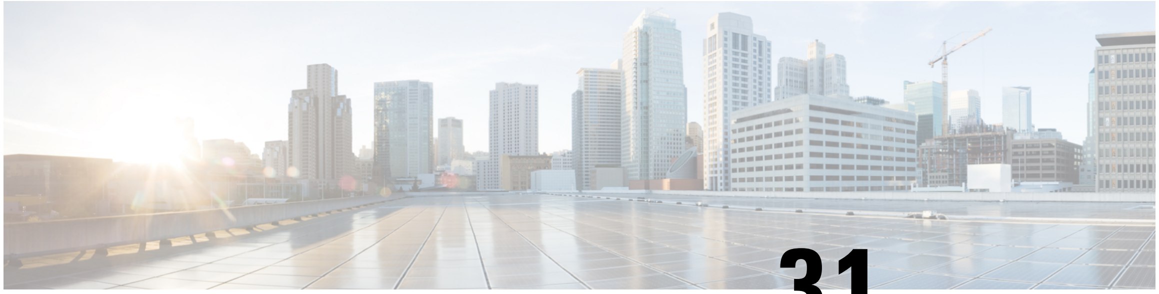
Step 3 **apply rack 0 slot** *slot number* **port***port number***propagate**

Example:

```
RP/0/RP0:hostname (config-fault-profile)# apply rack 0 slot LC2 port3 propagate
```

Loads the fault profile on the line card on port 3 of line card 2.

Step 4 **commit**



CHAPTER 31

Configuring PRBS

This chapter describes the procedure to configure the PRBS.

Configure PRBS

Procedure

Step 1 **exec**

Example:

```
Router> exec
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **terminal controller**

Example:

```
Router(config)# controller optics 0/15/0/2 port-mode otn framing opu2
```

Enters the global configuration mode.

Step 3 **secondary-admin-state**

Example:

```
Router(config)#controller odu2 0/15/0/2 secondary-admin-state maintenance
```

Enters the secondary admin state.

Step 4 **opu prbs mode {source|source-sink|sink} pattern {PN11|PN23|PN31|INVERTED_PN11|INVRTED_PN31}**

Example:

```
Router(config)# controller odu2 0/15/0/2 opu prbs mode source pattern pn31
```

Enters the attribute set in the path protection profile.

Step 5 **exit**

Example:

Router(config)# exit

Exits the controller configuration mode.

CHAPTER 32

Configuring Breakout

This chapter gives procedure to configure breakout.

Configure Breakout

Procedure

Step 1 **configure**

Step 2 **controller optics** *R/S/I/P*

Example:

```
RP/0/RP0:hostname (config)# controller optics 0/0/0/1
```

Enters the Optics controller mode.

Step 3 **otn framing** framing type

Example:

```
RP/0/RP0:hostname (config)# controller optics 0/0/0/1 breakout-mode 1 otn framing opu2
```

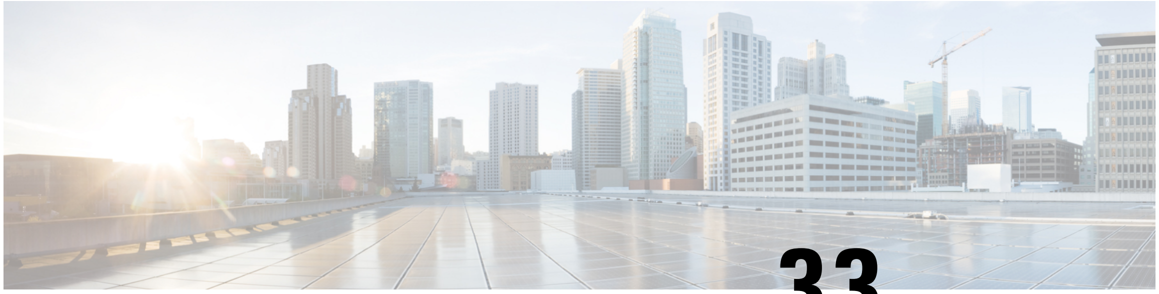
Configures OTN framing.

Step 4 **commit**

Example: Configure Breakout mode for Controller

The following example shows how to configure breakout-mode for a controller using Cisco IOS XR commands:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# controller optics 0/0/0/1
RP/0/RP0:hostname(config)# controller optics 0/0/0/1 breakout-mode 1
RP/0/RP0:hostname(config)# controller optics 0/0/0/1 breakout-mode 1 otn framing opu2
RP/0/RP0:hostname(config-otu1)#commit
```



CHAPTER 33

Configure High Availability1

This chapter describes the procedures for fast recovery of the system from various faults that can occur in any part of the network.

Card Reload

Perform this task to reload a card.

Procedure

hw-module location *value* **reload**

Example:

```
RP/0/RP0:hostname # hw-module location 0/2 reload
```

Note Only sysadmin can run this command.

Enters the location name to reload the card.

Redundancy Switchover

Perform this task to switchover from active LC/RP VM to standby LC/RP VM.

Procedure

redundancy switchover location *value*

Example:

```
RP/0/RP0:hostname # redundancy switchover location 0/RP1
```

```
RP/0/RP0:hostname # redundancy switchover location 0/LC0
```

Note If Frequency Synchronization is configured on the node, it will take up to 60 seconds to attain the frequency synchronization lock after VM switchover.

Process Restart

Perform this task to restart the process.

Procedure

process restart job id *value*

Example:

```
RP/0/RP0:hostname # process restart job id 53
```

Enters the job id to restarts the process.

CHAPTER 34

Configure Layer 3 VPNs

This chapter describes Layer 3 QinQ and the procedures to configure Layer 3 QinQ.

Table 30: Feature History

Feature Name	Release Information	Feature Description
Dual tag for L3VPN on dataplane for inBand management	Cisco IOS XR Release 6.5.31	The Layer 3 QinQ feature allows you to increase the number of VLAN tags in an interface and increment the number of subinterfaces up to 4094. Hence, with the dual tag, the number of VLANs can reach up to 4094*4094. You can enable this feature either on a physical interface or on a bundle interface. Commands modified: • encapsulation dot1q

Layer 3 QinQ

The Layer 3 QinQ feature enables you to increase the number of VLAN tags in an interface and increment the number of subinterfaces up to 4094. Hence, with the dual tag, the number of VLANs can reach up to 4094*4094. You can enable this feature either on a physical interface or on a bundle interface. When you cofigure this feature with the dual tag, interfaces check for IP addresses along with MAC addresses. Layer 3 QinQ is an extension of IEEE 802.1 QinQ VLAN tag stacking.

A dot1q VLAN subinterface is a virtual interface that is associated with a VLAN ID on a routed physical interface or a bundle interface. Subinterfaces divide the parent interface into two or more virtual interfaces. You can assign unique Layer 3 parameters on these virtual interfaces, such as IP addresses and dynamic routing protocols. The IP address for each subinterface must be in a different subnet from any other subinterface on the parent interface.

This feature supports:

- 802.1Q standards like 0x8100, 0x9100, 0x9200 (used as outer tag ether-type) and 0x8100 (used as inner tag ether-type).
- L3 802.1ad VLAN subinterfaces with 0x88a8 as the outer S-tag ether-type.
- Coexistence of Layer 2 and Layer 3 single tagged and double tagged VLANs.
- QinQ and dot1ad over Ethernet bundle subinterfaces.

The Layer 3 QinQ feature allows you to provision quality of service (QoS), access lists (ACLs), bidirectional forwarding detection (BFD), NetFlow, routing protocols, and IPv4 unicast and multicast.

Table 31: Types of Subinterfaces

Interface Type	Outer Tag	Inner Tag
Dot1q subinterface	0x8100	None
QinQ subinterface	0x8100	0x8100
QinQ subinterface	0x88a8	0x8100
QinQ subinterface	0x9100	0x8100
QinQ subinterface	0x9200	0x8100

QoS on Layer 3 VPN

Table 32: Feature History

Feature Name	Release Information	Feature Description
QoS on Layer 3 VPN.	Cisco IOS XR Release 6.5.33	The L3VPN QoS support on NCS4000 brings the Uniform and Pipe tunneling modes for DSCP/MPLS experimental bits, while the packet travels from one customer edge (CE) router to another across the MPLS core. The tunneling modes allow the customers to set the priority of the IP packets for the MPLS and the core networks.

QoS enables tunneling to be transparent from one edge of a network to the other edge of the network. A tunnel starts where there is label imposition and ends where the label is disposed off. Label disposition is where the label is removed from the stack. The removed packet goes out as an MPLS packet with a different per-hop behavior (PHB) layer underneath or as an IP packet with the IP PHB layer.

Packets are forwarded in the following three ways through a network with respect to QoS.

- **Uniform Tunneling Mode** In the Uniform Tunneling mode, packets are treated uniformly in the IP and MPLS networks, that is, the IP Precedence value and the MPLS EXP bits always are identical. Whenever a router changes or recolors the PHB of a packet, that change must be propagated to all encapsulation markings. The propagation is performed by a router only when a PHB is added or exposed due to label imposition or disposition on any router in the packet's path. The color must be reflected everywhere, at all levels.
- **Pipe Tunneling Mode**
- **Short Pipe Tunneling Mode**

Pipe mode and Short Pipe mode provide QoS transparency. With QoS transparency, the customer's IP marking in the IP packet is preserved.

Note QoS transparency does not support short Pipe mode in this release.

Uniform mode is the default Tunneling Mode available on NCS4K. In this mode, the DiffServ Code Point/MPLS Experimental (EXP) bits as the packet travels from one customer edge (CE) router to another CE router across the MPLS core is as follows:

To implement the pipe tunneling mode, Conditional marking of MPLS experimental bits and DSCP preservation for L3VPN Traffic are enabled.

Conditional Marking of MPLS experimental bits for L3VPN Traffic

The conditional marking of MPLS experimental bits is achieved for Layer 3 VPN traffic by applying a combination of ingress and egress policy maps on the provider edge (PE) router. In the ingress policy map, the QoS-group or discard class is set either based on the result of the policing action or implicitly. The egress policy map matches on qos-group or discard-class and sets the MPLS experiment bits to the corresponding value.

Conditional marking of the MPLS experimental bits is done differently for in-contract and out-of-contract packets. In-contract packets are the confirmed packets with the color green and discard-class set to 0. Out-of-contract packets have exceeded the limit and have the color yellow and discard class set to 1.

Conditional marking of MPLS experimental bits for L3VPN can be done on physical and bundle main interfaces and subinterfaces.

The DSCP value of the IP packet is preserved for L3VPN networks when the experimental remarking is done on the imposition node. The original IP DSCP value is preserved on the disposition node, and egress queuing is done based on MPLS EXP.

Tunneling Pipe Mode

Tunneling Pipe Mode uses two layers of QoS:

- An underlying QoS for the data, which remains unchanged when traversing the core.
- A per-core QoS, which is separate from that of the underlying IP packets. This per-core QoS pre-hop behavior(PHB) remains transparent to end users.

When a packet reaches the edge of the MPLS core, the egress PE router (PE2) classifies the newly exposed IP packets for outbound queuing based on the MPLS PHB from the EXP bits of the recently removed label.

Additional capabilities across Imposition-PE, Core-P, and Disposition-PE nodes are enabled to enable the Functional requirements of Uniform and Pipe tunneling mode.

Imposition-PE

Following Capabilities are enabled in Imposition-PE:

- Supports implicit copy of precedence or DSCP to experimental bits (default mode)
- Supports explicit marking of experimental bits on ingress or egress
- Supports condition experimental bits marking on egress
- Classification based on L4 protocol

Core-P

Following Capabilities are enabled in Core-P:

- Supports no experimental bits remarking (default mode)
- Set MPLS top most at ingress

Disposition-PE

Following Capabilities are enabled in Disposition-PE:

- Experimental bits not copied to DSCP (Default mode)
- Classification on experimental bits in ingress for egress queuing support (pipe mode)

The following is a sample configuration of no experimental bits marking at ingress.

```
1.Configs at PE-1 (no EXP marking, dscp copied to EXP at imposition)
a.Ingress policy:
class-map prec3
    match precedence 3
end-class-map

policy-map ingressPE1
    class prec3
      set traffic-class 3
end-policy-map

b.Egress policy:
class-map tc3
   match traffic-class 3
end-class-map

policy-map egressPE1
   class tc3
      shape average percent 10
end-policy-map

2.Configs at P (swapping the label)
a.Ingress policy
class-map mpls-in-exp3
  match mpls experimental topmost 3
end-class-map
```

```
policy-map mpls-in-pol
  class mpls-in-exp3
   set mpls experimental topmost 2
end-policy-map

3.Configs at PE 2 (EXP not copied to dscp of exposed IP packet)
a.Ingress policy
class-map mpls-in-exp2
    match mpls experimental topmost 2
end-class-map

policy-map ing-PE2
   class mpls-in-exp2
     set traffic-class 2
end-policy-map

b.Egress policy
class-map tc2
match traffic-class 2
end-policy-map

policy-map egr-PE2
   class tc2
     shape average percent 10
end-policy-map
```

The following is a sample configuration of experimental bits marking at ingress.

```
1.Configs at PE-1 (setting the EXP label - imposition)
a.Ingress policy:
class-map dscpcs3
    match dscp cs3
end-class-map

policy-map ingressPE1
    class dscpcs3
      set qos-group 2
end-policy-map

b.Egress policy:
class-map qgrp2
   match qos-group 2
end-class-map

policy-map egressPE1
   class-map qgrp2
      set mpls experimental imposition 4
end-policy-map

2.Configs at P (swapping the label)
a.Ingress policy

class-map mpls-in-exp4
  match mpls experimental topmost 4
end-class-map

policy-map mpls-in-pol-P1
  class mpls-in-exp4
   set mpls experimental topmost 5
 end-policy-map

3.Configs at PE 2 (outgoing queueing policy)
a.Ingress policy
class-map mpls-in-exp5
    match mpls experimental topmost 5
```

```
end-class-map

policy-map ing-PE2
   class mpls-in-exp5
     set traffic-class 3
end-policy-map

b.Egress policy

class-map tc3
   match traffic-class 3
end-class-map

policy-map egr-PE2
   class tc3
     shape average percent 10
end-policy-map
```

The following is a sample configuration of conditional experimental bits marking at ingress.

```
1.Configs at PE-1 (conditional EXP marking at egress)
a.Ingress policy:
class-map dscpcs3
    match dscp cs3
end-class-map

policy-map ing-PE1
    class dscpcs3
      set qos-group 2
set traffic-class 2
police rate percent 5 peak-rate percent 10
end-policy-map

b.Egress policy:

class-map match-all qgrp2dc1
   match qos-group 2
   match discard-class 1
end-class-map

class-map match-all qgrp2dc0
  match qos-group 2
  match discard-class 0
end-class-map

class-map tc2
  match traffic-class 2
end-class-map

policy-map egr-mark-PE1
   class qgrp2dc1
      set mpls experimental imposition 4
   class qgrp2dc0
      set mpls experimental imposition 6
end-policy-map

policy-map egr-shape-PE1
  class tc2
     shape average percent 5
end-policy-map


2.Configs at P (swapping the label)
a.Ingress policy
```

```
class-map mpls-in-exp4
  match mpls experimental topmost 4
end-class-map

policy-map mpls-in-pol-P1
  class mpls-in-exp4
   set mpls experimental topmost 5
 end-policy-map

3.Configs at PE 2 (outgoing queueing policy)
a.Ingress policy

class-map mpls-in-exp5
    match mpls experimental topmost 5
end-class-map

class-map mpls-in-exp6
    match mpls experimental topmost 6
end-class-map

policy-map ing-PE2
   class mpls-in-exp5
     set traffic-class 3
   class mpls-in-exp6
     set traffic-class 4
end-policy-map

b.Egress policy:
class-map tc3
   match traffic-class 3
end-class-map

class-map tc4
   match traffic-class 4
end-class-map

policy-map egr-PE2
   class tc3
     shape average percent 10
   class tc4
     shape average percent 5
end-policy-map
```

Configuration and Software Restrictions

- In the ingress policy map, if qos-group is set for the incoming traffic packets, then the setting of DSCP and MPLS experimental bits will not work. In other words, set experimental bits/DSCP and set QoS-group cannot be used together. Setting MPLS experimental bits, precedence or DSCP, and QoS-group in the same class on ingress, the result is unpredictable on egress when used for the match.

- Both the ingress and egress policy maps must be applied to attain the expected behavior. If either one of them is not applied, then it might lead to undefined behavior.

- When access control list and QoS co-exist on an interface, the QoS statistics don’t work, whereas the ACL stats always works. When the ACL is removed from the interface, QoS statistics start working.

- All the control traffic hits Class Traffic 6 by default due to the DNX design, we cannot change the queuing.

Configure Layer 3 QinQ

Perform this task to configure the Layer 3 QinQ feature.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface Bundle-Ether1000.3
RP/0/RP0:hostname(config-subif)# ipv4 address 192.0.2.1/24
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 3 second-dot1q 4000
RP/0/RP0:hostname(config-subif)# commit
```

Verify Layer 3 QinQ

This section shows the verification of Layer 3 QinQ configuration.

```
RP/0/# show interfaces Bundle-Ether1000.3
Bundle-Ether1000.3 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 0c75.bd30.1c88
  Internet address is 192.0.2.1/24
  MTU 1522 bytes, BW 30000000 Kbit (Max: 30000000 Kbit)
     reliability 255/255, txload 0/255, rxload 6/255
  Encapsulation 802.1Q Virtual LAN, VLAN Id 3, 2nd VLAN Id 4000,
  loopback not set,
  Last link flapped 19:30:41
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:01:59
  Last clearing of "show interface" counters never
  5 minute input rate 797298000 bits/sec, 844605 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     59288018302 packets input, 6995904900380 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 2 broadcast packets, 516 multicast packets
     419 packets output, 54968 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
```

CHAPTER 35

Configure Flex LSP

This chapter describes the Cisco IOS XR commands to configure Flex LSP.

Flex LSP Overview

Flex LSP also known as Associated Bidirectional LSPs is the combination of static bidirectional MPLS-TP and dynamic MPLS-TE. Flex LSP provides bidirectional label switched paths (LSPs) set up dynamically through Resource Reservation Protocol–Traffic Engineering (RSVP-TE). It does not support non-co routed LSPs.

Flex Label Switched Paths are LSP instances where the forward and the reverse direction paths are setup, monitored and protected independently and associated together during signaling. You use a RSVP Association object to bind the two forward and reverse LSPs together to form a co-routed associated bidirectional TE tunnel.

You can associate a protecting MPLS-TE tunnel with either a working MPLS-TE LSP, protecting MPLS-TE LSP, or both. The working LSP is the primary LSP backed up by the protecting LSP. When a working LSP goes down, the protecting LSP is automatically activated. You can configure a MPLS-TE tunnel to operate without protection as well.

Signaling Methods and Object Association for Flex LSPs

This section provides an overview of the association signaling methods for the bidirectional LSPs. Two unidirectional LSPs can be bound to form an associated bidirectional LSP in the following scenarios:

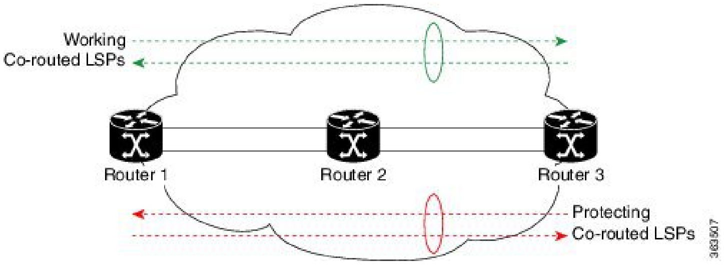
- No unidirectional LSP exists, and both must be established.
- Both unidirectional LSPs exist, but the association must be established.
- One unidirectional LSP exists, but the reverse associated LSP must be established.

Associated Bidirectional Co-routed LSPs

This section provides an overview of associated bidirectional co-routed LSPs. Establishment of MPLS TE-LSP involves computation of a path between a head-end node to a tail-end node, signaling along the path, and modification of intermediate nodes along the path. The signaling process ensures bandwidth reservation (if signaled bandwidth is lesser than 0 and programming of forwarding entries).

Path computation is performed by the head-end nodes of both the participating LSPs using Constrained Shortest Path First (CSPF). CSPF is the 'shortest path (measured in terms of cost) that satisfies all relevant LSP TE constraints or attributes, such as required bandwidth, priority and so on.

Associated Bidirectional Co-routed LSPs: A co-routed bidirectional TE LSP denotes a bidirectional tunnel where the forward direction LSP and reverse direction LSP must follow the same path, for example, the same nodes and paths. Here is an illustration.



In the above topology:

- Paths at the top of the figure (in green) indicate working co-routed LSP pairs.
- Paths at the bottom of the figure (in red) indicate protecting co-routed LSP pairs.
- Router 1 sets up working LSP to Router 3 (in green) after performing bidirectional CSPF and sends reverse explicit route object (ERO) to Router 3. Node Router 3 uses the received reverse ERO to set up reverse green working LSP to Router 1.
- Router 3 sets up protecting LSP to Router 1 (in red) after performing bidirectional CSPF and sends reverse ERO to Router 1. Node Router 1 uses the received reverse ERO to set up reverse red protecting LSP to Router 3.

Restrictions for Flex LSP

- Exp-null over Flex-LSP is not supported.
- 50 msec convergence is not guaranteed without WRAP protection. WRAP protection is mandatory to achieve 50 msec convergence for remote failures.
- TE NSR and IGP NSR are mandatory for RSP switchover.
- VPLS over Flex-LSP is not supported.
- Non-co routed Flex LSP is not supported.
- Sub interface shut will not guarantee 50 msec convergence.
- MPLS forwarding table stats is not supported.

- 1000 tunnels are supported with wrap protection and path protection.

Key Features supported in Flex LSP

Following list outlines key features supported:

- **Protection -**

  Following Protection features are supported:

  - **Lockout:** Using Lockout feature, user can perform lockout protection on a selected LSP and can switch traffic to protecting LSP, if the selected LSP carries the traffic. LSP on locked out interface remains up but no traffic flows on the locked out path. To configure lockout under an MPLS-TE enabled interface:

    ```
    RP/0/RP0:hostname# configure
    RP/0/RP0:hostname(config)# mpls traffic-eng
    RP/0/RP0:hostname(config-mpls-te)# interface tenGigE0/1/0/1
    RP/0/RP0:hostname(config-mpls-te-if)# fault-oam lockout
    ```

  - **Wrap Protection:** Using Wrap Protection, each LSP signals unique wrap label for head-end to identify lookback traffic and sends it over protect LSP. To configure Wrap Protection:

    ```
    RP/0/RP0:hostname# configure
    RP/0/RP0:hostname(config)# interface tunnel-te1
    RP/0/RP0:hostname(config-if)# ipv4 unnumbered Loopback0
    RP/0/RP0:hostname(config-if)# destination 49.49.49.2
    RP/0/RP0:hostname(config-if)# path-option 10 explicit name PATH1-2-3
    RP/0/RP0:hostname(config-if)# bidirectional association id 100 source-address
    49.49.49.2
    RP/0/RP0:hostname(config-if)# bidirectional association association type co-routed
    RP/0/RP0:hostname(config-if)# wrap-protection
    RP/0/RP0:hostname(config-if)# fault-oam
    ```

- **MPLS-OAM:** MPLS-OAM supports single segment pseudowire going over the associated bidirectional TE tunnels. This support includes pseudowires signaled dynamically, statically, or using a mix of both modes. To configure MPLS-OAM, use the following command:

  ```
  RP/0/RP0:hostname# configure
  RP/0/RP0:hostname(config)# mpls oam
  RP/0/RP0:hostname(config-oam)# echo reply-mode control-channel allow-reverse-lsp
  ```

  Following features are supported:

  - **LSP Ping:** Using LSP ping, use can enable on demand ping. It supports IP encapsulation for both request and reply messages. It also performs reverse path verification.

    Following is the example of LSP Ping configuration:

    ```
    RP/0/RP0:hostname# ping mpls traffic-eng tunnel-te 1 reply mode control-channel

    Tue May 21 11:04:12.211 EDT
    Sending 5, 100-byte MPLS Echos to tunnel-te1,
          timeout is 2 seconds, send interval is 0 msec:

    Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
    ```

```
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
```

- **Traceroute:** Traceroute supports IP-encapsulation but not for echo reply. Following is the example of Traceroute configuration:

```
RP/0/RP0:hostname# traceroute mpls traffic-eng tunnel-te 1

Tue May 21 11:06:16.056 EDT
Tracing MPLS TE Label Switched Path on tunnel-te1, timeout is 2 seconds

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

Type escape sequence to abort.

  0 10.10.10.1 MRU 1500 [Labels: 16005 Exp: 0]
L 1 10.10.10.2 MRU 1500 [Labels: implicit-null Exp: 0] 11 ms
! 2 13.13.13.4 4 ms
```

- **Protecting LSP reoptimization:** Changes to the protecting LSP are performed using a tear and resetup mechanism. When protecting LSP changes are in progress there will be a window during which the tunnel is unprotected and working LSP failures will result in traffic loss.

Note This feature is applicable only for bidirectional co-routed tunnels.

- **SRLG-Aware Path Protection :** This feature specifies that a protecting LSP should be SRLG-diverse from the primary LSP. The user can also specify node-diversity.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)#interface tunnel-te 100
RP/0/RP0:hostname(config-if)#path-protection srlg-diverse
RP/0/RP0:hostname(config-if)#
```

- **Sticky Paths:** This feature allows tunnels to maintain a constant path through the network using dynamic path-options. It applies to both working and protected LSP's and it is an extension of the lockdown property. Sticky paths persist across a tunnel-down event and a sticky LSP that goes down will not come back up until the original path is available.

  Following example shows how a configuration switch is added to the path-option configuration to enable sticky paths:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te 1
RP/0/RP0:hostname(config-if)# path-option 1
RP/0/RP0:hostname(config-if)# path-option 1 dynamic lockdown sticky
```

Following example shows how to verify the sticky path configuration:

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


Name: tunnel-te1  Destination: 192.168.0.2  Ifhandle:0xd0
Signalled-Name: XR_A_t1
Status:
    Admin:    up Oper:   up (Uptime 2d19h)

    path option 10, (LOCKDOWN STICKY) type dynamic  (Basis for Setup, path weight 9
(reverse 9))
      Accumulative metrics: TE 9 (reverse 9) IGP 9 (reverse 9) Delay 300000 (reverse
300000)
      Protected-by PO index: 20
      Bandwidth:    30000 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
      Metric Type: TE (global)
      Path Selection:
        Tiebreaker: Min-fill (default)
      Hop-limit: disabled
      Cost-limit: disabled
      Delay-limit: disabled
      Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    path option 20, (LOCKDOWN STICKY) type dynamic  (Basis for Standby, path weight 10
 (reverse 10))
     Accumulative metrics: TE 10 (reverse 10) IGP 10 (reverse 10) Delay 300000 (reverse
 300000)
      Bandwidth:    30000 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
      Metric Type: TE (global)
      Path Selection:
        Tiebreaker: Min-fill (default)
      Hop-limit: disabled
      Cost-limit: disabled
      Delay-limit: disabled
      Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 30000 kbps  CT0
    Creation Time: Mon Feb 26 15:35:17 2018 (2d19h ago)
  Config Parameters:
    Bandwidth:    30000 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (global)
    Path Selection:
      Tiebreaker: Min-fill (default)
    Hop-limit: disabled
    Cost-limit: disabled
    Delay-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    AutoRoute:  enabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (not enabled)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
Auto-Capacity: Disabled:
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Enabled
      Diversity: node, SRLG
      Non-revertive
    Association Type: Single Sided Bidirectional LSPs, Co-routed: YES
    Association ID: 1, Source: 192.168.0.1, Global ID: 1
    Reverse Bandwidth: 30000 kbps (CT0), Standby: 30000 kbps (CT0)
    LSP Wrap Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    Soft Preemption: Disabled
  History:
    Tunnel has been up for: 2d19h (since Mon Feb 26 15:36:20 EST 2018)
    Current LSP:
      Uptime: 2d18h (since Mon Feb 26 16:35:15 EST 2018)
    Reopt. LSP:
      Last Failure:
        LSP not signalled, identical to the [CURRENT] LSP
        Date/Time: Thu Mar 01 02:35:15 EST 2018 [08:30:59 ago]
    Standby Reopt LSP:
      Last Failure:
        LSP not signalled, identical to the [STANDBY] LSP
        Date/Time: Thu Mar 01 02:35:15 EST 2018 [08:30:59 ago]
        First Destination Failed: 192.168.0.2
    Prior LSP:
      ID: 2 Path Option: 20
      Removal Trigger: reoptimization completed
    Standby LSP:
      Uptime: 00:01:01 (since Thu Mar 01 11:05:13 EST 2018)

  Path info (OSPF 100 area 0):
  Node hop count: 1
  Hop0: 10.10.10.2
  Hop1: 192.168.0.2

  Standby LSP Path info (OSPF 100 area 0), Oper State: Up :
  Node hop count: 1
  Hop0: 11.11.11.2
  Hop1: 192.168.0.2

  Sticky working path:
    Path-option 10
    Node hop count: 1
    Hop0: 10.10.10.2
Hop1: 192.168.0.2

  Sticky protecting path:
    Path-option 20
    Node hop count: 1
    Hop0: 11.11.11.2
    Hop1: 192.168.0.2
s
```

Follwing example shows how to clear sticky paths and trigger reoptimization of a specified tunnel. :

```
RP/0/RP0:hostname#mpls traffic-eng reroute name t1
```

- **Non-revertive (NRV) Behavior:** In case of failure, no new working LSP is established and traffic remains on the protecting LSP. Recovery occurs only in response to user intervention or in event of failure of the protecting path.

  Following example shows how to add a configuration switch to the path-protection configuration and hence enable NRV behavior:

```
  RP/0/RP0:hostname # configure
  RP/0/RP0:hostname(config)# interface tunnel-te 1
  RP/0/RP0:hostname(config-if)# path-protection
  RP/0/RP0:hostname(config-if)# protection-mode non-revertive
```

Following example shows how the existing mpls traffic-eng switchover command is extended for NRV recovery:

```
RP/0/RP0:hostname# mpls traffic-eng path-protection switchover non-revertive tunnel-name
 t1
```

- **Path Protection Switch Over (PPSO) Recovery:**

  PPSO is the XR path-protection recovery mechanism. It is now compliant with the standards and can interop with XE.

- **Interoperability:** A compatibility configuration switch is added to enable interoperability with XE platform. This switch exists on a per-tunnel basis and is not backward compatible with XR. Enabling or disabling this switch on a tunnel results in tunnel flap. Following is the example of compatibility switch configuration:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-if)# bidirectional
RP/0/RP0:hostname(config-if-bidir)# association type co-routed
RP/0/RP0:hostname(config-if-bidir-co-routed)# signaling protection-object  disable


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

Association:
       Association Type: Single Sided Bidirectional LSPs (Tie breaking slave)
       Association ID: 999, Source: 192.168.0.4
     Extended Association:
       Global source: 0
       Extended ID:
         0xc0a80003 0x2 0x0 0x0
       Decoded Extended ID:
         Master source address: 192.168.0.3
         Master LSP-ID: 2
         Master protecting LSP-ID: 0
         Flags: 0x0 (BFD FALSE, NRV FALSE, restore-lsp FALSE)
```

Flex LSP Scale Details

Scale details for Flex LSP:

Table 33: Supported LSPs for FLex LSP

Flex LSP with wrap protection	Head/Tail Node: 18750 LSPs Mid Node: 12500 LSPs
Flex LSP without wrap protection	Head/Tail Node: 18750 LSPs Mid Node: 75000 LSPs

How to Configure Co-routed Flex LSPs

A co-routed bidirectional packet LSP is a combination of two LSPs (one in the forward direction and the other in reverse direction) sharing the same path between a pair of ingress and egress nodes. It is established using the extensions to RSVP-TE. This type of LSP can be used to carry any of the standard types of MPLS-based traffic, including Layer 2 VPNs.

The configuration includes the following steps:

1. Enable basic MPLS Traffic Engineering on hostname PE1 and RSVP Configuration.
2. Configure Flex LSP.
3. Enable Wrap Protection.
4. Enable Fault OAM.
5. Map pseudowire to a specific Flex LSP tunnel.

Configuring Co-routed Flex LSPs

Before you begin

- You must have symmetric source and destination TE router IDs in order for bidirectional LSPs to be associated.
- Tunnels attributes must be configured identically on both sides of co-routed bidirectional LSP.

Note Up to 1000 Flex LSP tunnels are supported.

Procedure

1. Enable basic MPLS Traffic Engineering on hostname PE1 and RSVP Configuration:

Configure MPLS-TE;

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)# interface TenGigE0/9/0/0/12.1
```

Configure RSVP:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# rsvp
RP/0/RP0:hostname(config-rsvp)# signalling hello graceful-restart refresh interval 3000
RP/0/RP0:hostname(config-rsvp)# interface TenGigE0/8/0/0/102.1 bandwidth 1000000
RP/0/RP0:hostname(config-rsvp)# interface TenGigE0/5/0/4.1 bandwidth 1000000
```

2. Configure Flex LSP:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-if)# ipv4 unnumbered Loopback0
RP/0/RP0:hostname(config-if)# destination 49.49.49.2
RP/0/RP0:hostname(config-if)# path-option 10 explicit name PATH1-2-3
RP/0/RP0:hostname(config-if)# bidirectional
RP/0/RP0:hostname(config-if-bidir)# association id 100 source-address 49.49.49.2
RP/0/RP0:hostname(config-if-bidir-co-routed)# association type co-routed
```

3. Wrap Protection:

For Wrap Protection:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-if)# ipv4 unnumbered Loopback0
RP/0/RP0:hostname(config-if)# destination 49.49.49.2
RP/0/RP0:hostname(config-if)# path-option 10 explicit name PATH1-2-3
RP/0/RP0:hostname(config-if)# bidirectional
RP/0/RP0:hostname(config-if-bidir)# association id 100 source-address 49.49.49.2
RP/0/RP0:hostname(config-if-bidir)# association type co-routed
RP/0/RP0:hostname(config-if-bidir-co-routed)# wrap-protection
```

4. Enable Fault OAM

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface tunnel-te1
RP/0/RP0:hostname(config-if)# ipv4 unnumbered Loopback0
RP/0/RP0:hostname(config-if)# destination 49.49.49.2
RP/0/RP0:hostname(config-if)# path-option 10 explicit name PATH1-2-3
RP/0/RP0:hostname(config-if)# bidirectional
RP/0/RP0:hostname(config-if-bidir)# association id 100 source-address 49.49.49.2
RP/0/RP0:hostname(config-if-bidir)# association type co-routed
RP/0/RP0:hostname(config-if-bidir-co-routed)# fault-oam
```

5. Map pseudowire to a specific Flex LSP tunnel:

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# pw-class foo
RP/0/RP0:hostname(config-l2vpn-pwc)# encapsulation mpls
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)# preferred-path interface tunnel-te 1
RP/0/RP0:hostname(config-l2vpn-pwc)# exit
RP/0/RP0:hostname(config-l2vpn)# exit
RP/0/RP0:hostname(config-l2vpn)# xconnect group gold
RP/0/RP0:hostname(config-l2vpn-xc)# p2p cust_one
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor ipv4 49.49.49.2 pw-id 1
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class foo
```

Verifying the Co-routed Flex LSP Configuration

To verify the co-routed LSP, use the **show mpls traffic-eng tunnels detail** command.

```
RP/0/RP0:hostname# show mpls traffic-eng tunnels 7001 detail

Name: tunnel-te7001  Destination: 104.0.0.1  Ifhandle:0x8000aa4
  Signalled-Name: NCS4K-R11_t7001
  Status:
    Admin:    up Oper:   up (Uptime 136y10w)

    path option 1,  type explicit path01 (Basis for Setup, path weight 30 (reverse 30))
      Protected-by PO index: 2
    path option 2,  type explicit path02 (Basis for Standby, path weight 100010 (reverse
100010))
      Protected-by PO index: 1
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 10 kbps  CT0
    Creation Time: Wed Jan 11 03:08:36 2017 (136y10w 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: Disabled, Protection Desired: None
    Path Protection: Enabled
    Association Type: Single Sided Bidirectional LSPs, Co-routed: YES
    Association ID: 86, Source: 192.0.0.0
    Reverse Bandwidth: 10 kbps (CT0), Standby: 10 kbps (CT0)
    LSP Wrap Protection: Enabled

    Reoptimization after affinity failure: Enabled
    Soft Preemption: Disabled
  Fault-OAM Info:
    Last Fault Msg: Clear
  SNMP Index: 25
  Binding SID: None
  Path Protection Info:
    Standby Path: User defined [explicit path option: 2],
    Last Switchover:
      136y10w ago, From LSP 14 To LSP 16
      No subcause recorded
      Reopt time remaining: 0 seconds
    Number of Switchovers 1, Standby Ready 3 times, Standby Reopt 0 times
    Lockout Info:
      Locked Out: NO
      Locked out LSP ID: 0
      Lockout Originated By: None
    LSP Wrap Protection: Enabled
      LSP Wrap Label: 24182
  History:
    Reopt. LSP:
      Last Failure:
        LSP not signalled, identical to the [CURRENT] LSP
        Date/Time: Tue Jan 10 21:42:41 UTC 2017 [00:03:42 ago]
    Standby Reopt LSP:
```

```
    Last Failure:
      LSP not signalled, identical to the [STANDBY] LSP
      Date/Time: Tue Jan 10 21:42:41 UTC 2017 [00:03:42 ago]
      First Destination Failed: 104.0.0.1
  Prior LSP:
    ID: 14 Path Option: 1
    Removal Trigger: path protection switchover
Current LSP Info:
  Instance: 18, Signaling Area: IS-IS 100 level-2
  Uptime: 136y10w (since Wed Jan 11 03:09:56 UTC 2017)
  Outgoing Interface: TenGigE0/4/0/2.1, Outgoing Label: 24157
  Router-IDs: local      102.0.0.1
              downstream 107.0.0.1
  Soft Preemption: None
  SRLGs: not collected
  Path Info:
    Outgoing:
      Explicit Route:
        Strict, 1.27.1.2
        Strict, 3.67.1.2
        Strict, 3.67.1.1
        Strict, 1.46.1.2
        Strict, 1.46.1.1
        Strict, 104.0.0.1

    Record Route: Disabled
    Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
    Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
                        Soft Preemption Desired: Not Set
    Reverse Associated LSP Information:
      Signaled Name: NCS4K-R10_t7001
      Tunnel: 7001, Source: 104.0.0.1, Dest: 102.0.0.1, LSP: 9, State: Up
    Association:
      Association Type: Single Sided Bidirectional LSPs
      Association ID: 86, Source: 192.0.0.0
    Extended Association:
      Global source: 0
      Extended ID:
        0x66000001 (102.0.0.1)
        0x12 (0.0.0.18)
    Protection:
      Secondary (S): 0, Protecting (P): 0, Notification (N): 0, Oper (O): 0
      Link Flags: Any, LSP Flags: 1:N Protection with Extra-Traffic
    Reverse Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
    Reverse ERO:
      Explicit Route:
        Strict, 1.46.1.1
        Strict, 1.46.1.2
        Strict, 3.67.1.1
        Strict, 3.67.1.2
        Strict, 1.27.1.2
        Strict, 1.27.1.1
        Strict, 102.0.0.1

  Resv Info: None
    Record Route: Disabled
    Fspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
Standby LSP Info:
  Instance: 19, Signaling Area: IS-IS 100 level-2
  Uptime: 136y10w (since Wed Jan 11 03:10:04 UTC 2017), Oper State: Up
  Outgoing Interface: TenGigE0/4/0/11.1, Outgoing Label: 24176
  Router-IDs: local      102.0.0.1
              downstream 109.0.0.1
  Soft Preemption: None
```

```
    SRLGs: not collected
    Path Info:
      Outgoing:
        Explicit Route:
          Strict, 1.29.1.2
          Strict, 1.49.1.2
          Strict, 1.49.1.1
          Strict, 104.0.0.1

      Record Route: Disabled
      Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
                          Soft Preemption Desired: Not Set
      Reverse Associated LSP Information:
        Signaled Name: NCS4K-R10_t7001
        Tunnel: 7001, Source: 104.0.0.1, Dest: 102.0.0.1, LSP: 10, State: Up
      Association:
        Association Type: Single Sided Bidirectional LSPs
        Association ID: 86, Source: 192.0.0.0
      Extended Association:
        Global source: 0
        Extended ID:
          0x68000001 (104.0.0.1)
          0xa (0.0.0.10)
      Protection:
        Secondary (S): 0, Protecting (P): 1, Notification (N): 0, Oper (O): 0
        Link Flags: Any, LSP Flags: 1:N Protection with Extra-Traffic
    Resv Info: None
      Record Route: Disabled
      Fspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
  Persistent Forwarding Statistics:
    Out Bytes: 20272384
    Out Packets: 79189

LSP Tunnel 104.0.0.1 7001 [9] is signalled, Signaling State: up
  Tunnel Name: NCS4K-R10_t7001 Tunnel Role: Tail
  InLabel: TenGigE0/4/0/2.1, 24164
  Signalling Info:
    Src 104.0.0.1 Dst 102.0.0.1, Tun ID 7001, Tun Inst 9, 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: 1.27.1.1
      Incoming:
      Explicit Route:
        Strict, 1.27.1.1
        Strict, 102.0.0.1

      Record Route: Disabled
      Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
                          Soft Preemption Desired: Not Set
      Reverse Associated LSP Information:
        Signaled Name: NCS4K-R11_t7001
        Tunnel: 7001, Source: 102.0.0.1, Dest: 104.0.0.1, LSP: 18, State: Up
      Association:
        Association Type: Single Sided Bidirectional LSPs (Tie breaking slave)
        Association ID: 86, Source: 192.0.0.0
      Extended Association:
        Global source: 0
        Extended ID:
          0x66000001 (102.0.0.1)
          0x12 (0.0.0.18)
      Protection:
        Secondary (S): 0, Protecting (P): 0, Notification (N): 0, Oper (O): 0
        Link Flags: Any, LSP Flags: 1:N Protection with Extra-Traffic
    Resv Info: None
      Record Route: Disabled
      Fspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits

LSP Tunnel 104.0.0.1 7001 [10] is signalled, Signaling State: up
  Tunnel Name: NCS4K-R10_t7001 Tunnel Role: Tail
  InLabel: TenGigE0/4/0/11.1, 24463
  Signalling Info:
    Src 104.0.0.1 Dst 102.0.0.1, Tun ID 7001, Tun Inst 10, Ext ID 104.0.0.1
    Router-IDs: upstream   109.0.0.1
                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: 1.29.1.1
      Incoming:
      Explicit Route:
        Strict, 1.29.1.1
        Strict, 102.0.0.1

      Record Route: Disabled
      Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
                          Soft Preemption Desired: Not Set
      Reverse Associated LSP Information:
        Signaled Name: NCS4K-R11_t7001
        Tunnel: 7001, Source: 102.0.0.1, Dest: 104.0.0.1, LSP: 19, State: Up
      Association:
        Association Type: Single Sided Bidirectional LSPs (Tie breaking slave)
        Association ID: 86, Source: 192.0.0.0
      Extended Association:   Fspec: avg rate=8K, burst=1K, peak rate=8K
```

To verify the forwarding interface, use the **show mpls forwarding tunnels detail** command.

```
RP/0/RP0:hostname# show mpls forwarding tunnels 7001 detail

Tunnel        Outgoing    Outgoing     Next Hop        Bytes
Name          Label       Interface                    Switched
------------- ----------- ------------ --------------- ------------
tt7001            24157       Te0/4/0/2.1  1.27.1.2        0
     Updated: Jan 10 21:40:04.966
     Version: 17852, Priority: 2
     Label Stack (Top -> Bottom): { 24157 }
     Local Label: 24354
     NHID: 0x0, Encap-ID: INVALID, Path idx: 0, Backup path idx: 0, Weight: 0
     MAC/Encaps: 18/22, MTU: 1500
     Packets Switched: 0

  Interface Name: tunnel-te7001, Interface Handle: 0x08000aa4, Local Label: 24354
  Forwarding Class: 0, Weight: 0
  Packets/Bytes Switched: 79189/20272384
```

CHAPTER 36

Configure ISIS

This chapter describes the Cisco IOS XR commands to configure ISIS.

Prerequisites for Implementing IS-IS

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.

Restrictions for Implementing IS-IS

When multiple instances of IS-IS are being run, an interface can be associated with only one instance (process). Instances may not share an interface.

Information About Implementing IS-IS

To implement IS-IS you need to understand the following concepts:

IS-IS Functional Overview

Small IS-IS networks are typically built as a single area that includes all routers in the network. As the network grows larger, it may be reorganized into a backbone area made up of the connected set of all Level 2 routers from all areas, which is in turn connected to local areas. Within a local area, routers know how to reach all system IDs. Between areas, routers know how to reach the backbone, and the backbone routers know how to reach other areas.

The IS-IS routing protocol supports the configuration of backbone Level 2 and Level 1 areas and the necessary support for moving routing information between the areas. Routers establish Level 1 adjacencies to perform routing within a local area (intra-area routing). Routers establish Level 2 adjacencies to perform routing between Level 1 areas (interarea routing).

Each IS-IS instance can support either a single Level 1 or Level 2 area, or one of each. By default, all IS-IS instances automatically support Level 1 and Level 2 routing. You can change the level of routing to be performed by a particular routing instance using the **is-type** command.

Restrictions

When multiple instances of IS-IS are being run, an interface can be associated with only one instance (process). Instances may not share an interface.

Key Features Supported in the IS-IS Implementation

The following list outlines key features supported in the implementation:

- Multitopology
- Nonstop forwarding (NSF), both Cisco proprietary and IETF
- Three-way handshake
- Mesh groups
- Multiple IS-IS instances
- Configuration of a broadcast medium connecting two networking devices as a point-to-point link
- Fast-flooding with different threads handling flooding and shortest path first (SPF).

IS-IS Configuration Grouping

Cisco IOS XR groups all of the IS-IS configuration in router IS-IS configuration mode, including the portion of the interface configurations associated with IS-IS. To display the IS-IS configuration in its entirety, use the **show running router isis** command. The command output displays the running configuration for all configured IS-IS instances, including the interface assignments and interface attributes.

IS-IS Configuration Modes

The following sections show how to enter each of the configuration modes. From a mode, you can enter the **?** command to display the commands available in that mode.

Router Configuration Mode

The following example shows how to enter router configuration mode:

```
RP/0/RP0::hostname# configuration
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)#
```

Router Address Family Configuration Mode

The following example shows how to enter router address family configuration mode:

```
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)#
```

Interface Configuration Mode

The following example shows how to enter interface configuration mode:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-isis-if)#
```

Interface Address Family Configuration Mode

The following example shows how to enter interface address family configuration mode:

```
RP/0/RP0:hostname(config)# router isis isp
RP/0/RP0:hostname(config-isis)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-if-af)#
```

IS-IS Interfaces

IS-IS interfaces can be configured as one of the following types:

- Active—advertises connected prefixes and forms adjacencies. This is the default for interfaces.
- Passive—advertises connected prefixes but does not form adjacencies. The **passive** command is used to configure interfaces as passive. Passive interfaces should be used sparingly for important prefixes such as loopback addresses that need to be injected into the IS-IS domain. If many connected prefixes need to be advertised then the redistribution of connected routes with the appropriate policy should be used instead.
- Suppressed—does not advertise connected prefixes but forms adjacencies. The **suppress** command is used to configure interfaces as suppressed.
- Shutdown—does not advertise connected prefixes and does not form adjacencies. The **shutdown** command is used to disable interfaces without removing the IS-IS configuration.

Limit LSP Flooding

Limiting link-state packets (LSP) may be desirable in certain “meshy” network topologies. An example of such a network might be a highly redundant one such as a fully meshed set of point-to-point links over a nonbroadcast multiaccess (NBMA) transport. In such networks, full LSP flooding can limit network scalability. One way to restrict the size of the flooding domain is to introduce hierarchy by using multiple Level 1 areas and a Level 2 area. However, two other techniques can be used instead of or with hierarchy: Block flooding on specific interfaces and configure mesh groups.

Both techniques operate by restricting the flooding of LSPs in some fashion. A direct consequence is that although scalability of the network is improved, the reliability of the network (in the face of failures) is reduced because a series of failures may prevent LSPs from being flooded throughout the network, even though links exist that would allow flooding if blocking or mesh groups had not restricted their use. In such a case, the link-state databases of different routers in the network may no longer be synchronized. Consequences such as persistent forwarding loops can ensue. For this reason, we recommend that blocking or mesh groups be used only if specifically required, and then only after careful network design.

Flood Blocking on Specific Interfaces

With this technique, certain interfaces are blocked from being used for flooding LSPs, but the remaining interfaces operate normally for flooding. This technique is simple to understand and configure, but may be more difficult to maintain and more error prone than mesh groups in the long run. The flooding topology that IS-IS uses is fine-tuned rather than restricted. Restricting the topology too much (blocking too many interfaces) makes the network unreliable in the face of failures. Restricting the topology too little (blocking too few interfaces) may fail to achieve the desired scalability.

To improve the robustness of the network in the event that all nonblocked interfaces drop, use the **csnp-interval** command in interface configuration mode to force periodic complete sequence number PDUs (CSNPs) packets to be used on blocked point-to-point links. The use of periodic CSNPs enables the network to become synchronized.

Mesh Group Configuration

Configuring mesh groups (a set of interfaces on a router) can help to limit flooding. All routers reachable over the interfaces in a particular mesh group are assumed to be densely connected with each router having at least one link to every other router. Many links can fail without isolating one or more routers from the network.

In normal flooding, a new LSP is received on an interface and is flooded out over all other interfaces on the router. With mesh groups, when a new LSP is received over an interface that is part of a mesh group, the new LSP is not flooded over the other interfaces that are part of that mesh group.

Maximum LSP Lifetime and Refresh Interval

By default, the router sends a periodic LSP refresh every 15 minutes. LSPs remain in a database for 20 minutes by default. If they are not refreshed by that time, they are deleted. You can change the LSP refresh interval or maximum LSP lifetime. The LSP interval should be less than the LSP lifetime or else LSPs time out before they are refreshed. In the absence of a configured refresh interval, the software adjusts the LSP refresh interval, if necessary, to prevent the LSPs from timing out.

IS-IS Authentication

Authentication is available to limit the establishment of adjacencies by using the **hello-password** command, and to limit the exchange of LSPs by using the **lsp-password** command.

IS-IS supports plain-text authentication, which does not provide security against unauthorized users. Plain-text authentication allows you to configure a password to prevent unauthorized networking devices from forming adjacencies with the router. The password is exchanged as plain text and is potentially visible to an agent able to view the IS-IS packets.

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.

IS-IS stores a configured password using simple encryption. However, the plain-text form of the password is used in LSPs, sequence number protocols (SNPs), and hello packets, which would be visible to a process that can view IS-IS packets. The passwords can be entered in plain text (clear) or encrypted form.

To set the domain password, configure the **lsp-password** command for Level 2; to set the area password, configure the **lsp-password** command for Level 1.

The keychain feature allows IS-IS to reference configured keychains. IS-IS key chains enable hello and LSP keychain authentication. Keychains can be configured at the router level (in the case of the **lsp-password** command) and at the interface level (in the case of the **hello-password** command) within IS-IS. These commands reference the global keychain configuration and instruct the IS-IS protocol to obtain security parameters from the global set of configured keychains.

IS-IS is able to use the keychain to implement hitless key rollover for authentication. Key rollover specification is time based, and in the event of clock skew between the peers, the rollover process is impacted. The configurable tolerance specification allows for the accept window to be extended (before and after) by that margin. This accept window facilitates a hitless key rollover for applications (for example, routing and management protocols).

Nonstop Forwarding

On software, NSF minimizes the amount of time a network is unavailable to its users following a route processor (RP) failover. The main objective of NSF is to continue forwarding IP packets and perform a graceful restart following an RP failover.

When a router restarts, all routing peers of that device usually detect that the device went down and then came back up. This transition results in what is called a *routing flap*, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. NSF helps to suppress routing flaps in NSF-aware devices, thus reducing network instability.

NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following an RP failover. When the NSF feature is configured, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards while the standby RP assumes control from the failed active RP during a failover. The ability of line cards to remain up through a failover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.

When the Cisco IOS XR router running IS-IS routing performs an RP failover, the router must perform two tasks to resynchronize its link-state database with its IS-IS neighbors. First, it must relearn the available IS-IS neighbors on the network without causing a reset of the neighbor relationship. Second, it must reacquire the contents of the link-state database for the network.

The IS-IS NSF feature offers two options when configuring NSF:

- IETF NSF
- Cisco NSF

If neighbor routers on a network segment are NSF aware, meaning that neighbor routers are running a software version that supports the IETF Internet draft for router restartability, they assist an IETF NSF router that is restarting. With IETF NSF, neighbor routers provide adjacency and link-state information to help rebuild the routing information following a failover.

Cisco NSF checkpoints (stores persistently) all the state necessary to recover from a restart without requiring any special cooperation from neighboring routers. The state is recovered from the neighboring routers, but only using the standard features of the IS-IS routing protocol. This capability makes Cisco NSF suitable for use in networks in which other routers have not used the IETF standard implementation of NSF.

Note If you configure IETF NSF on the Cisco IOS XR router and a neighbor router does not support IETF NSF, the affected adjacencies flap, but nonstop forwarding is maintained to all neighbors that do support IETF NSF. A restart reverts to a cold start if no neighbors support IETF NSF.

Multi-Instance IS-IS

You can configure up to eight IS-IS instances. MPLS can run on multiple IS-IS processes as long as the processes run on different sets of interfaces. Each interface may be associated with only a single IS-IS instance. Cisco IOS XR software prevents the double-booking of an interface by two instances at configuration time—two instances of MPLS configuration causes an error.

Because the Routing Information Base (RIB) treats each of the IS-IS instances as equal routing clients, you must be careful when redistributing routes between IS-IS instances. The RIB does not know to prefer Level 1 routes over Level 2 routes. For this reason, if you are running Level 1 and Level 2 instances, you must enforce the preference by configuring different administrative distances for the two instances.

Multiprotocol Label Switching Traffic Engineering

The MPLS TE feature enables an MPLS backbone to replicate and expand the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies.

For IS-IS, MPLS TE automatically establishes and maintains MPLS TE label-switched paths across the backbone by using Resource Reservation Protocol (RSVP). The route that a label-switched path uses is determined by the label-switched paths resource requirements and network resources, such as bandwidth. Available resources are flooded by using special IS-IS TLV extensions in the IS-IS. The label-switched paths are explicit routes and are referred to as traffic engineering (TE) tunnels.

Overload Bit on Router

The overload bit is a special bit of state information that is included in an LSP of the router. If the bit is set on the router, it notifies routers in the area that the router is not available for transit traffic. This capability is useful in four situations:

1. During a serious but nonfatal error, such as limited memory.
2. During the startup and restart of the process. The overload bit can be set until the routing protocol has converged. However, it is not employed during a normal NSF restart or failover because doing so causes a routing flap.
3. During a trial deployment of a new router. The overload bit can be set until deployment is verified, then cleared.
4. During the shutdown of a router. The overload bit can be set to remove the router from the topology before the router is removed from service.

Overload Bit Configuration During Multitopology Operation

Because the overload bit applies to forwarding for a single topology, it may be configured and cleared independently for IPv4 during multitopology operation. For this reason, the overload is set from the router address family configuration mode. If the IPv4 overload bit is set, all routers in the area do not use the router for IPv4 transit traffic.

IS-IS Overload Bit Avoidance

The IS-IS overload bit avoidance feature allows network administrators to prevent label switched paths (LSPs) from being disabled when a router in that path has its Intermediate System-to-Intermediate System (IS-IS) overload bit set.

When the IS-IS overload bit avoidance feature is activated, all nodes with the overload bit set, including head nodes, mid nodes, and tail nodes, are ignored, which means that they are still available for use with label switched paths (LSPs).

Note The IS-IS overload bit avoidance feature does *not* change the default behavior on nodes that have their overload bit set if those nodes are not included in the path calculation (PCALC).

The IS-IS overload bit avoidance feature is activated using the following command:

mpls traffic-eng path-selection ignore overload

The IS-IS overload bit avoidance feature is deactivated using the **no** form of this command:

no mpls traffic-eng path-selection ignore overload

When the IS-IS overload bit avoidance feature is deactivated, nodes with the overload bit set cannot be used as nodes of last resort.

Default Routes

You can force a default route into an IS-IS routing domain. Whenever you specifically configure redistribution of routes into an IS-IS routing domain, the software does not, by default, redistribute the default route into the IS-IS routing domain. The **default-information originate** command generates a *default route* into IS-IS, which can be controlled by a route policy. You can use the route policy to identify the level into which the default route is to be announced, and you can specify other filtering options configurable under a route policy. You can use a route policy to conditionally advertise the default route, depending on the existence of another route in the routing table of the router.

Attached Bit on an IS-IS Instance

The attached bit is set in a router that is configured with the **is-type** command and **level-1-2** keyword. The attached bit indicates that the router is connected to other areas (typically through the backbone). This functionality means that the router can be used by Level 1 routers in the area as the default route to the backbone. The attached bit is usually set automatically as the router discovers other areas while computing its Level 2 SPF route. The bit is automatically cleared when the router becomes detached from the backbone.

Note If the connectivity for the Level 2 instance is lost, the attached bit in the Level 1 instance LSP would continue sending traffic to the Level 2 instance and cause the traffic to be dropped.

To simulate this behavior when using multiple processes to represent the **level-1-2** keyword functionality, you would manually configure the attached bit on the Level 1 process.

IS-IS Support for Route Tags

The IS-IS Support for route tags feature provides the capability to associate and advertise a tag with an IS-IS route prefix. Additionally, the feature allows you to prioritize the order of installation of route prefixes in the RIB based on a tag of a route. Route tags may also be used in route policy to match route prefixes (for example, to select certain route prefixes for redistribution).

MPLS TE Forwarding Adjacency

MPLS TE forwarding adjacency allows a network administrator to handle a traffic engineering, label switch path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network, based on the Shortest Path First (SPF) algorithm. A forwarding adjacency can be created between routers in the same IS-IS level. The routers can be located multiple hops from each other. As a result, a TE tunnel is advertised as a link in an IGP network, with the cost of the link associated with it. Routers outside of the TE domain see the TE tunnel and use it to compute the shortest path for routing traffic throughout the network.

MPLS TE forwarding adjacency is considered in IS-IS SPF only if a two-way connectivity check is achieved. This is possible if the forwarding adjacency is bidirectional or the head end and tail end routers of the MPLS TE tunnel are adjacent.

The MPLS TE forwarding adjacency feature is supported by IS-IS. For details on configuring MPLS TE forwarding adjacency, see the MPLS Configuration Guide.

MPLS TE Interarea Tunnels

MPLS TE interarea tunnels allow you to establish MPLS TE tunnels that span multiple IGP areas (Open Shorted Path First [OSPF]) and levels (IS-IS), removing the restriction that required that both the tunnel headend and tailend routers be in the same area. The IGP can be either IS-IS or OSPF. See the Configuring MPLS Traffic Engineering for IS-IS, on page 376 for information on configuring MPLS TE for IS-IS.

For details on configuring MPLS TE interarea tunnels, see the MPLS Configuration Guide.

Unequal Cost Multipath Load-balancing for IS-IS

The unequal cost multipath (UCMP) load-balancing adds the capability with intermediate system-to-intermediate system (IS-IS) to load-balance traffic proportionally across multiple paths, with different cost.

Generally, higher bandwidth links have lower IGP metrics configured, so that they form the shortest IGP paths. With the UCMP load-balancing enabled, IGP can use even lower bandwidth links or higher cost links for traffic, and can install these paths to the forwarding information base (FIB). IS-IS IGP still installs multiple paths to the same destination in FIB, but each path will have a 'load metric/weight' associated with it. FIB uses this load metric/weight to decide the amount of traffic that needs to be sent on a higher bandwidth path and the amount of traffic that needs to be sent on a lower bandwidth path.

The UCMP computation is provided under IS-IS per address family, enabling UCMP computation for a particular address family. The UCMP configuration is also provided with a prefix-list option, which would limit the UCMP computation only for the prefixes present in the prefix-list. If prefix-list option is not provided, UCMP computation is done for the reachable prefixes in IS-IS. The number of UCMP nexthops to be considered and installed is controlled using the **variance** configuration. Variance value identifies the range for the UCMP path metric to be considered for installation into routing information base (RIB) and is defined in terms of a percentage of the primary path metric. Total number of paths, including ECMP and UCMP paths together is limited by the max-path configuration or by the max-path capability of the platform.

Enabling the UCMP configuration indicates that IS-IS should perform UCMP computation for the all the reachable ISIS prefixes or all the prefixes in the prefix-list, if the prefix-list option is used. The UCMP computation happens only after the primary SPF and route calculation is completed. There would be a delay of ISIS_UCMP_INITIAL_DELAY (default delay is 100 ms) milliseconds from the time route calculation is completed and UCMP computation is started. UCMP computation will be done before fast re-route computation. Fast re-route backup paths will be calculated for both the primary equal cost multipath (ECMP) paths and the UCMP paths. Use the **ucmp delay-interval** command to configure the delay between primary SPF completion and start of UCMP computation.

UCMP ratio can be adjusted by any of the following ways:

- By using the **bandwidth** command in interface configuration mode .
- By adjusting ISIS metric on the links.

There is an option to exclude an interface from being used for UCMP computation. If it is desired that a particular interface should not be considered as a UCMP nexthop, for any prefix, then use the **ucmp exclude interface** command to configure the interface to be excluded from UCMP computation.

Enabling IS-IS and Configuring Level 1 or Level 2 Routing

This task explains how to enable IS-IS and configure the routing level for an area.

Note Configuring the routing level in Step 4 is optional, but is highly recommended to establish the proper level of adjacencies.

Before you begin

Although you can configure IS-IS before you configure an IP address, no IS-IS routing occurs until at least one IP address is configured.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- By default, all IS-IS instances are automatically Level 1 and Level 2. You can change the level of routing to be performed by a particular routing instance by using the **is-type** router configuration command.

Step 3 **net** *network-entity-title*

Example:

```
RP/0/RP0:hostname(config-isis)# net 47.0004.004d.0001.0001.0c11.1110.00
```

Configures network entity titles (NETs) for the routing instance.

- Specify a NET for each routing instance if you are configuring multi-instance IS-IS.
- This example configures a router with area ID 47.0004.004d.0001 and system ID 0001.0c11.1110.00.
- To specify more than one area address, specify additional NETs. Although the area address portion of the NET differs, the systemID portion of the NET must match exactly for all of the configured items.

Step 4 **is-type** { **level-1** | **level-1-2** | **level-2-only** }

Example:

```
RP/0/RP0:hostname(config-isis)# is-type level-2-only
```

(Optional) Configures the system type (area or backbone router).

- By default, every IS-IS instance acts as a **level-1-2** router.
- The **level-1** keyword configures the software to perform Level 1 (intra-area) routing only. Only Level 1 adjacencies are established. The software learns about destinations inside its area only. Any packets containing destinations outside the area are sent to the nearest **level-1-2** router in the area.
- The **level-2-only** keyword configures the software to perform Level 2 (backbone) routing only, and the router establishes only Level 2 adjacencies, either with other Level 2-only routers or with **level-1-2** routers.
- The **level-1-2** keyword configures the software to perform both Level 1 and Level 2 routing. Both Level 1 and Level 2 adjacencies are established. The router acts as a border router between the Level 2 backbone and its Level 1 area.

Step 5 **commit**

Step 6 **show isis** [**instance** *instance-id*] **protocol**

Example:

```
RP/0/RP0:hostname# show isis protocol
```

(Optional) Displays summary information about the IS-IS instance.

Configuring Single Topology for IS-IS

After an IS-IS instance is enabled, it must be configured to compute routes for a specific network topology.

This task explains how to configure the operation of the IS-IS protocol on an interface for an IPv4 topology.

Before you begin

Note To enable the router to run in single-topology mode, configure each of the IS-IS interfaces with all of the address families enabled and “single-topology” in the address-family unicast in the IS-IS router stanza. You can use the IPv4 address family, but your configuration must represent the set of all active address families on the router.

Two exceptions to these instructions exist:

1. If the address-family stanza in the IS-IS process contains the **adjacency-check disable** command, then an interface is not required to have the address family enabled.
2. The **single-topology** command is not valid in the ipv4 address-family submode.

The default metric style for single topology is narrow metrics. However, you can use either wide metrics or narrow metrics. How to configure them depends on how single topology is configured.

Procedure

Step 1 **configure**

Step 2 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/3
```

Enters interface configuration mode.

Step 3 Do one of the following:

- **ipv4 address** *address mask*

Example:

```
RP/0/RP0:hostname(config-if)# ipv4 address 10.0.1.3 255.255.255.0
```

or

Defines the IPv4 address for the interface. An IP address is required on all interfaces in an area enabled for IS-IS if any one interface is configured for IS-IS routing.

- The link-local address can be used only to communicate with nodes on the same link.

Step 4 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration mode, and returns the router to XR config mode.

Step 5 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- By default, all IS-IS instances are Level 1 and Level 2. You can change the level of routing to be performed by a particular routing instance by using the **is-type** command.

Step 6 **net** *network-entity-title*

Example:

```
RP/0/RP0:hostname(config-isis)# net 47.0004.004d.0001.0001.0c11.1110.00
```

Configures NETs for the routing instance.

- Specify a NET for each routing instance if you are configuring multi-instance IS-IS. You can specify a name for a NET and for an address.
- This example configures a router with area ID 47.0004.004d.0001 and system ID 0001.0c11.1110.00.
- To specify more than one area address, specify additional NETs. Although the area address portion of the NET differs, the system ID portion of the NET must match exactly for all of the configured items.

Step 7 **single-topology**

Example:

```
RP/0/RP0:hostname(config-isis-af)# single-topology
```

Step 8 exit

Example:

```
RP/0/RP0:hostname(config-isis-af)# exit
```

Exits router address family configuration mode, and returns the router to router configuration mode.

Step 9 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/1/0/3
```

Enters interface configuration mode.

Step 10 **circuit-type** { **level-1** | **level-1-2** | **level-2-only** }

Example:

```
RP/0/RP0:hostname(config-isis-if)# circuit-type level-1-2
```

(Optional) Configures the type of adjacency.

- The default circuit type is the configured system type (configured through the **is-type** command).
- Typically, the circuit type must be configured when the router is configured as only **level-1-2** and you want to constrain an interface to form only **level-1** or **level-2-only** adjacencies.

Step 11 **address-family** **ipv4**]

Example:

```
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
```

Specifies the IPv4 address family, and enters interface address family configuration mode.

- This example specifies the unicast IPv4 address family on the interface.

Step 12 **commit**

Step 13 **show isis** [**instance** *instance-id*] **interface** [*type interface-path-id*] [**detail**] [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname# show isis interface TenGigE 0/1/0/1
```

(Optional) Displays information about the IS-IS interface.

Step 14 **show isis** [**instance** *instance-id*] **topology** [**systemid** *system-id*] [**level** { **1** | **2** }] [**summary**]

Example:

```
RP/0/RP0:hostname# show isis topology
```

(Optional) Displays a list of connected routers in all areas.

Configuring Multitopology Routing

This set of procedures configures multitopology routing, which is used by PIM for reverse-path forwarding (RPF) path selection.

Restrictions for Configuring Multitopology Routing

- Only the default VRF is currently supported in a multitopology solution.
- Only intermediate system-intermediate system (IS-IS) routing protocols are currently supported.
- Topology selection is restricted solely to (S, G) route sources for both SM and SSM. Static and IS-IS are the only interior gateway protocols (IGPs) that support multitopology deployment.

  For non-(S, G) route sources like a rendezvous point or bootstrap router (BSR), or when a route policy is not configured, the current policy default remains in effect. In other words, a unicast-default table is selected for all sources, based on OSFP/IS-IS/Multiprotocol Border Gateway Protocol (MBGP) configuration.

Information About Multitopology Routing

Configuring multitopology networks requires the following tasks:

Configuring a Global Topology and Associating It with an Interface

Follow these steps to enable a global topology in the default VRF and to enable its use with a specific interface.

Procedure

Step 1 **configure**

Step 2 **address-family** { **ipv4** } *topo-name*

Example:

```
RP/0/RP0:hostname(config)# address-family ipv4 topology green
```

Configures a topology in the default VRF table that will be associated with a an interface.

Step 3 **maximum prefix** *limit*

Example:

```
RP/0/RP0:hostname(config-af)# maximum prefix 100
```

(Optional) Limits the number of prefixes allowed in a topology routing table. Range is 32 to 2000000.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-af)# interface TenGigE 0/3/0/0
```

Specifies the interface to be associated with the previously specified VRF table that will add the connected and local routes to the appropriate routing table.

Step 5 **address-family** { **ipv4** } *topo-name*

Example:

```
RP/0/RP0:hostname(config-if)# address-family ipv4 unicast topology green
```

Enables the topology for the interface specified in Configuring a Global Topology and Associating It with an Interface, on page 366, adding the connected and local routes to the appropriate routing table.

Step 6 Repeat Step 4 and Step 5 until you have specified all the interface instances you want to associate with your topologies.

Example:

```
RP/0/RP0:hostname(config-if-af)# interface TenGigE 0/3/2/0
RP/0/RP0:hostnamerouter(config-if)# address-family ipv4 unicast topology purple
RP/0/RP0:hostname(config-if-af)#
```

Step 7 **commit**

Enabling an IS-IS Topology

To enable a topology in IS-IS, you must associate an IS-IS topology ID with the named topology. IS-IS uses the topology ID to differentiate topologies in the domain.

Note This command must be configured prior to other topology commands.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis purple
```

Enters IS-IS configuration submode.

Step 3 **address-family** { **ipv4** } *topo-name*

Example:

```
RP/0/RP0:hostname(config-isis)# address-family ipv4 topology green
```

Associates an IS-IS topology ID with the named topology.

Step 4 **topology-id** *toplogy-id*

Example:

```
RP/0/RP0:hostname(config-isis-af)# topology-id 122
```

Step 5 **commit**

Placing an Interface in a Topology in IS-IS

To associate an interface with a topology in IS-IS, follow these steps.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis purple
```

Enters IS-IS configuration submode.

Step 3 **net** *network-entity-title*

Example:

```
RP/0/RP0:hostname(config-isis)# net netname
```

Creates a network entity title for the configured isis interface.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/3/0/0
```

Enters isis interface configuration submode and creates an interface instance.

Step 5 **address-family** { **ipv4** *topo-name*

Example:

```
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 topology green
```

- Enters isis address-family interface configuration submode.
- Places the interface instance into a topology.

Step 6 Repeat Placing an Interface in a Topology in IS-IS, on page 367 and Placing an Interface in a Topology in IS-IS, on page 367 until you have specified all the interface instances and associated topologies you want to configure in your network.

—

Step 7 **commit**

Configuring a Routing Policy

Procedure

Step 1 **configure**

Step 2 **route-policy** *policy-name*

Example:

```
RP/0/RP0:hostname(config)# route-policy mt1
RP/0/RP0:hostname(config-rpl)# if destination in 225.0.0.1, 225.0.0.11 then
RP/0/RP0:hostname(config-rpl-if)# if source in (10.10.10.10) then
RP/0/RP0:hostname(config-rpl-if-2)# set rpf-topology ipv4 topology greentable
RP/0/RP0:hostname(config-rpl-if-2)# else
RP/0/RP0:hostname(config-rpl-if-else-2)# set rpf-topology ipv4 topology bluetable
RP/0/RP0:hostname(config-rpl-if-else-2)# endif
RP/0/RP0:hostname(config-rpl-if)# endif
```

Defines a routing policy and enters routing policy configuration submode.

Step 3 **end-policy**

Example:

```
RP/0/RP0:hostname(config-rpl)# end-policy
RP/0/RP0:hostname(config)#
```

Signifies the end of route policy definition and exits routing policy configuration submode.

Step 4 **commit**

Configuring Multitopology for IS-IS

Multitopology is configured in the same way as the single topology. However, the **single - topology** command is omitted, invoking the default multitopology behavior. This task is optional.

Controlling LSP Flooding for IS-IS

Flooding of LSPs can limit network scalability. You can control LSP flooding by tuning your LSP database parameters on the router globally or on the interface. This task is optional.

Many of the commands to control LSP flooding contain an option to specify the level to which they apply. Without the option, the command applies to both levels. If an option is configured for one level, the other level continues to use the default value. To configure options for both levels, use the command twice. For example:

```
  RP/0/RP0:hostname(config-isis)# lsp-refresh-interval 1200 level 2
  RP/0/RP0:hostname(config-isis)# lsp-refresh-interval 1100 level 1
```

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- You can change the level of routing to be performed by a particular routing instance by using the **is-type** router configuration command.

Step 3 **lsp-refresh-interval** *seconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis)# lsp-refresh-interval 10800
```

(Optional) Sets the time between regeneration of LSPs that contain different sequence numbers

- The refresh interval should always be set lower than the **max-lsp-lifetime** command.

Step 4 **lsp-check-interval** *seconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis)# lsp-check-interval 240
```

(Optional) Configures the time between periodic checks of the entire database to validate the checksums of the LSPs in the database.

- This operation is costly in terms of CPU and so should be configured to occur infrequently.

Step 5 **lsp-gen-interval** { [**initial-wait** *initial* | **secondary-wait** *secondary* | **maximum-wait** *maximum*] ... } [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis)# lsp-gen-interval maximum-wait 15 initial-wait 5
```

(Optional) Reduces the rate of LSP generation during periods of instability in the network. Helps reduce the CPU load on the router and number of LSP transmissions to its IS-IS neighbors.

- During prolonged periods of network instability, repeated recalculation of LSPs can cause an increased CPU load on the local router. Further, the flooding of these recalculated LSPs to the other Intermediate Systems in the network causes increased traffic and can result in other routers having to spend more time running route calculations.

Step 6 **max-lsp-lifetime** *seconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis)# max-lsp-lifetime 11000
```

(Optional) Sets the initial lifetime given to an LSP originated by the router.

- This is the amount of time that the LSP persists in the database of a neighbor unless the LSP is regenerated or refreshed.

Step 7 **ignore-lsp-errors** **disable**

Example:

```
RP/0/RP0:hostname(config-isis)# ignore-lsp-errors disable
```

(Optional) Sets the router to purge LSPs received with checksum errors.

Step 8 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/1/0/3
```

Enters interface configuration mode.

Step 9 **lsp-interval** *milliseconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-if)# lsp-interval 100
```

(Optional) Configures the amount of time between each LSP sent on an interface.

Step 10 **csnp-interval** *seconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-if)# csnp-interval 30 level 1
```

(Optional) Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.

- Sending more frequent CSNPs means that adjacent routers must work harder to receive them.
- Sending less frequent CSNP means that differences in the adjacent routers may persist longer.

Step 11 **retransmit-interval** *seconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-if)# retransmit-interval 60
```

(Optional) Configures the amount of time that the sending router waits for an acknowledgment before it considers that the LSP was not received and subsequently resends.

```
RP/0/RP0:hostname(config-isis-if)# retransmit-interval 60
```

Step 12 **retransmit-throttle-interval** *milliseconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-if)# retransmit-throttle-interval 1000
```

(Optional) Configures the amount of time between retransmissions on each LSP on a point-to-point interface.

- This time is usually greater than or equal to the **lsp-interval** command time because the reason for lost LSPs may be that a neighboring router is busy. A longer interval gives the neighbor more time to receive transmissions.

Step 13 **mesh-group** { *number* | **blocked** }

Example:

```
RP/0/RP0:hostname(config-isis-if)# mesh-group blocked
```

(Optional) Optimizes LSP flooding in NBMA networks with highly meshed, point-to-point topologies.

- This command is appropriate only for an NBMA network with highly meshed, point-to-point topologies.

Step 14 **commit**

Step 15 **show isis interface** [*type interface-path-id* | **level** { **1** | **2** }] [**brief**]

Example:

```
RP/0/RP0:hostname# show isis interface TenGigE 0/1/0/1 brief
```

(Optional) Displays information about the IS-IS interface.

Step 16 **show isis** [**instance** *instance-id*] **database** [**level** { **1** | **2** }] [**detail** | **summary** | **verbose**] [***** | *lsp-id*]

Example:

```
RP/0/RP0:hostname# show isis database level 1
```

(Optional) Displays the IS-IS LSP database.

Step 17 **show isis** [**instance** *instance-id*] **lsp-log** [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname# show isis lsp-log
```

(Optional) Displays LSP log information.

Step 18 **show isis database-log** [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname# show isis database-log level 1
```

(Optional) Display IS-IS database log information.

Configuring Nonstop Forwarding for IS-IS

This task explains how to configure your router with NSF that allows to resynchronize the IS-IS link-state database with its IS-IS neighbors after a process restart. The process restart could be due to an:

- RP failover (for a warm restart)
- Simple process restart (due to an IS-IS reload or other administrative request to restart the process)
- IS-IS software upgrade

In all cases, NSF mitigates link flaps and loss of user sessions. This task is optional.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- You can change the level of routing to be performed by a particular routing instance by using the **is-type** router configuration command.

Step 3 **nsf** { **cisco** | **ietf** }

Example:

```
RP/0/RP0:hostname(config-isis)# nsf ietf
```

Enables NSF on the next restart.

- Enter the **cisco** keyword to run IS-IS in heterogeneous networks that might not have adjacent NSF-aware networking devices.
- Enter the **ietf** keyword to enable IS-IS in homogeneous networks where *all* adjacent networking devices support IETF draft-based restartability.

Step 4 **nsf interface-expires** *number*

Example:

```
RP/0/RP0:hostname(config-isis)# nsf interface-expires 1
```

Configures the number of resends of an acknowledged NSF-restart acknowledgment.

- If the resend limit is reached during the NSF restart, the restart falls back to a cold restart.

Step 5 **nsf interface-timer** *seconds*

Example:

```
RP/0/RP0:hostname(config-isis) nsf interface-timer 15
```

Configures the number of seconds to wait for each restart acknowledgment.

Step 6 **nsf lifetime** *seconds*

Example:

```
RP/0/RP0:hostname(config-isis)# nsf lifetime 20
```

Configures the maximum route lifetime following an NSF restart.

- This command should be configured to the length of time required to perform a full NSF restart because it is the amount of time that the Routing Information Base (RIB) retains the routes during the restart.
- Setting this value too high results in stale routes.
- Setting this value too low could result in routes purged too soon.

Step 7 **commit**

Step 8 **show running-config** [*command*]

Example:

```
RP/0/RP0:hostname# show running-config router isis isp
```

(Optional) Displays the entire contents of the currently running configuration file or a subset of that file.

- Verify that “nsf” appears in the IS-IS configuration of the NSF-aware device.

- This example shows the contents of the configuration file for the “isp” instance only.

Configuring Authentication for IS-IS

This task explains how to configure authentication for IS-IS. This task is optional.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- You can change the level of routing to be performed by a particular routing instance by using the **is-type** command.

Step 3 **lsp-password** { **hmac-md5** | **text** } { **clear** | **encrypted** } *password* [**level** { **1** | **2** }] [**send-only**] [**snp send-only**]

Example:

```
RP/0/RP0:hostname(config-isis)# lsp-password hmac-md5 clear password1 level 1
```

Configures the LSP authentication password.

- The **hmac-md5** keyword specifies that the password is used in HMAC-MD5 authentication.
- The **text** keyword specifies that the password uses cleartext password authentication.
- The **clear** keyword specifies that the password is unencrypted when entered.
- The **encrypted** keyword specifies that the password is encrypted using a two-way algorithm when entered.
- The **level 1** keyword sets a password for authentication in the area (in Level 1 LSPs and Level SNPs).
- The **level 2** keywords set a password for authentication in the backbone (the Level 2 area).
- The **send-only** keyword adds authentication to LSP and sequence number protocol data units (SNPs) when they are sent. It does not authenticate received LSPs or SNPs.
- The **snp send-only** keyword adds authentication to SNPs when they are sent. It does not authenticate received SNPs.

Note To disable SNP password checking, the **snp send-only** keywords must be specified in the **lsp-password** command.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-isis)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode.

Step 5 **hello-password** { **hmac-md5** | **text** } { **clear** | **encrypted** } *password* [**level** { **1** | **2** }] [**send-only**]

Example:

```
RP/0/RP0:hostname(config-isis-if)#hello-password text clear mypassword
```

Configures the authentication password for an IS-IS interface.

Step 6 **commit**

Configuring Keychains for IS-IS

This task explains how to configure keychains for IS-IS. This task is optional.

Keychains can be configured at the router level (**lsp-password** command) and at the interface level (**hello-password** command) within IS-IS. These commands reference the global keychain configuration and instruct the IS-IS protocol to obtain security parameters from the global set of configured keychains. The router-level configuration (**lsp-password** command) sets the keychain to be used for all IS-IS LSPs generated by this router, as well as for all Sequence Number Protocol Data Units (SN PDUs). The keychain used for HELLO PDUs is set at the interface level, and may be set differently for each interface configured for IS-IS.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- You can change the level of routing to be performed by a particular routing instance by using the **is-type** command.

Step 3 **l sp-password** **keychain** *keychain-name* [**level** { **1** | **2** }] [**send-only**] [**snp send-only**]

Example:

```
RP/0/RP0:hostname(config-isis)# lsp-password keychain isis_a level 1
```

Configures the keychain.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-isis)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode.

Step 5 **h ello-password keychain** *keychain-name* [**level** { **1** | **2** }] [**send-only**]

Example:

```
RP/0/RP0:hostname(config-isis-if)#hello-password keychain isis_b
```

Configures the authentication password for an IS-IS interface.

Step 6 **commit**

Configuring MPLS Traffic Engineering for IS-IS

This task explains how to configure IS-IS for MPLS TE. This task is optional.

Before you begin

Your network must support the MPLS software feature before you enable MPLS TE for IS-IS on your router.

Note You must enter the commands in the following task list on every IS-IS router in the traffic-engineered portion of your network.

Note MPLS traffic engineering currently does not support routing and signaling of LSPs over unnumbered IP links. Therefore, do not configure the feature over those links.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- You can change the level of routing to be performed by a particular routing instance by using the **is-type** router configuration command.

Step 3 **address-family** { **ipv4** } [**unicast**]

Example:

```
RP/0/RP0:hostname(config-isis)#address-family ipv4 unicast
```

Specifies the IPv4 address family, and enters router address family configuration mode.

Step 4 **mpls traffic-eng level** { **1** | **2** }

Example:

```
RP/0/RP0:hostname(config-isis-af)# mpls traffic-eng level 1
```

Configures a router running IS-IS to flood MPLS TE link information into the indicated IS-IS level.

Step 5 **mpls traffic-eng router-id** { *ip-address* | *interface-name interface-instance* }

Example:

```
RP/0/RP0:hostname(config-isis-af)# mpls traffic-eng router-id loopback0
```

Specifies that the MPLS TE router identifier for the node is the given IP address or an IP address associated with the given interface.

Step 6 **metric-style wide** [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-af)# metric-style wide level 1
```

Configures a router to generate and accept only wide link metrics in the Level 1 area.

Step 7 **commit**

Step 8 **show isis** [**instance** *instance-id*] **mpls traffic-eng tunnel**

Example:

```
RP/0/RP0:hostname# show isis instance isp mpls traffic-eng tunnel
```

(Optional) Displays MPLS TE tunnel information.

Step 9 **show isis** [**instance** *instance-id*] **mpls traffic-eng adjacency-log**

Example:

```
RP/0/RP0:hostname# show isis instance isp mpls traffic-eng adjacency-log
```

(Optional) Displays a log of MPLS TE IS-IS adjacency changes.

Step 10 **show isis** [**instance** *instance-id*] **mpls traffic-eng advertisements**

Example:

```
RP/0/RP0:hostname# show isis instance isp mpls traffic-eng advertisements
```

(Optional) Displays the latest flooded record from MPLS TE.

Tuning Adjacencies for IS-IS

This task explains how to enable logging of adjacency state changes, alter the timers for IS-IS adjacency packets, and display various aspects of adjacency state. Tuning your IS-IS adjacencies increases network stability when links are congested. This task is optional.

For point-to-point links, IS-IS sends only a single hello for Level 1 and Level 2, which means that the level modifiers are meaningless on point-to-point links. To modify hello parameters for a point-to-point interface, omit the specification of the level options.

The options configurable in the interface submode apply only to that interface. By default, the values are applied to both Level 1 and Level 2.

The **hello-password** command can be used to prevent adjacency formation with unauthorized or undesired routers. This ability is particularly useful on a LAN, where connections to routers with which you have no desire to establish adjacencies are commonly found.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- You can change the level of routing to be performed by a particular routing instance by using the **is-type** command.

Step 3 **log adjacency changes**

Example:

```
RP/0/RP0:hostname(config-isis)# log adjacency changes
```

Generates a log message when an IS-IS adjacency changes state (up or down).

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-isis)# interface TenGigE 0/1/0/3
```

Enters interface configuration mode.

Step 5 **hello-padding** { **disable** | **sometimes** } [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-if)# hello-padding sometimes
```

Configures padding on IS-IS hello PDUs for an IS-IS interface on the router.

- Hello padding applies to only this interface and not to all interfaces.

Step 6 **hello-interval** *seconds* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-if)#hello-interval 6
```

Specifies the length of time between hello packets that the software sends.

Step 7 **hello-multiplier** *multiplier* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-if)# hello-multiplier 10
```

Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.

- A higher value increases the networks tolerance for dropped packets, but also may increase the amount of time required to detect the failure of an adjacent router.
- Conversely, not detecting the failure of an adjacent router can result in greater packet loss.

Step 8 **h ello-password** { **hmac-md5** | **text** } { **clear** | **encrypted** } *password* [**level** { **1** | **2** }] [**send-only**]

Example:

```
RP/0/RP0:hostname(config-isis-if)# hello-password text clear mypassword
```

Specifies that this system include authentication in the hello packets and requires successful authentication of the hello packet from the neighbor to establish an adjacency.

Step 9 **commit**

Step 10 **show isis** [**instance** *instance-id*] **adjacency** *t ype* *interface- path-id*] [**detail**] [**systemid** *system-id*]

Example:

```
RP/0/RP0:hostname# show isis instance isp adjacency
```

(Optional) Displays IS-IS adjacencies.

Step 11 show isis adjacency-log

Example:

```
RP/0/RP0:hostname# show isis adjacency-log
```

(Optional) Displays a log of the most recent adjacency state transitions.

Step 12 **show isis** [**instance** *instance-id*] **interface** [*type* *interface-path-id*] [**brief** | **detail**] [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname# show isis interface TenGigE0/6/0/2.10 brief
```

(Optional) Displays information about the IS-IS interface.

Step 13 **show isis** [**instance** *instance-id*] **neighbors** [*interface-type* *interface-instance*] [**summary**] [**detail**] [**systemid** *system-id*]

Example:

```
RP/0/RP0:hostname# show isis neighbors summary
```

(Optional) Displays information about IS-IS neighbors.

Setting SPF Interval for a Single-Topology IPv4 Configuration

This task explains how to make adjustments to the SPF calculation to tune router performance. This task is optional.

Because the SPF calculation computes routes for a particular topology, the tuning attributes are located in the router address family configuration submode. SPF calculation computes routes for Level 1 and Level 2 separately.

To tune the SPF calculation parameters for single-topology mode, configure the **address-family ipv4 unicast** command.

The incremental SPF algorithm can be enabled separately. When enabled, the incremental shortest path first (ISPF) is not employed immediately. Instead, the full SPF algorithm is used to “seed” the state information required for the ISPF to run. The startup delay prevents the ISPF from running for a specified interval after an IS-IS restart (to permit the database to stabilize). After the startup delay elapses, the ISPF is principally responsible for performing all of the SPF calculations. The reseed interval enables a periodic running of the full SPF to ensure that the iSFP state remains synchronized.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing instance, and places the router in router configuration mode.

- You can change the level of routing to be performed by a particular routing instance by using the **is-type** router configuration command.

Step 3 **address-family** { **ipv4** } [**unicast**]

Example:

```
RP/0/RP0:hostname(config-isis)#address-family ipv4 unicast
```

Specifies the IPv4 address family, and enters router address family configuration mode.

Step 4 **spf-interval** {[**initial-wait** *initial* | **secondary-wait** *secondary* | **maximum-wait** *maximum*] ...} [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-af)# spf-interval initial-wait 10 maximum-wait 30
```

(Optional) Controls the minimum time between successive SPF calculations.

- This value imposes a delay in the SPF computation after an event trigger and enforces a minimum elapsed time between SPF runs.
- If this value is configured too low, the router can lose too many CPU resources when the network is unstable.
- Configuring the value too high delays changes in the network topology that result in lost packets.
- The SPF interval does not apply to the running of the ISPF because that algorithm runs immediately on receiving a changed LSP.

Step 5 **ispf** [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-af)# ispf
```

(Optional) Configures incremental IS-IS ISPF to calculate network topology.

Step 6 **commit**

Step 7 **show isis** [**instance** *instance-id*] [[**ipv4** | **afi-all**] [**unicast** | **safi-all**]] **spf-log** [**level** { **1** | **2** }] [**ispf** | **fspf** | **prc** | **nhc**] [**detail** | **verbose**] [**last** *number* | **first** *number*]

Example:

```
RP/0/RP0:hostname# show isis instance 1 spf-log ipv4
```

(Optional) Displays how often and why the router has run a full SPF calculation.

Customizing Routes for IS-IS

This task explains how to perform route functions that include injecting default routes into your IS-IS routing domain and redistributing routes learned in another IS-IS instance. This task is optional.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing process, and places the router in router configuration mode.

- By default, all IS-IS instances are automatically Level 1 and Level 2. You can change the level of routing to be performed by a particular routing instance by using the **is-type** command.

Step 3 **set-overload-bit** [**on-startup** { *delay* | **wait-for-bgp** }] [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis)# set-overload-bit
```

(Optional) Sets the overload bit.

Note The configured overload bit behavior does not apply to NSF restarts because the NSF restart does not set the overload bit during restart.

Step 4 **address-family** { **ipv4** } [**unicast**]

Example:

```
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
```

Specifies the IPv4 address family, and enters router address family configuration mode.

Step 5 **default-information originate** [**route-policy** *route-policy-name*]

Example:

```
RP/0/RP0:hostname(config-isis-af)# default-information originate
```

(Optional) Injects a default IPv4 route into an IS-IS routing domain.

- The **route-policy** keyword and *route-policy-name* argument specify the conditions under which the IPv4 default route is advertised.
- If the **route-policy** keyword is omitted, then the IPv4 default route is unconditionally advertised at Level 2.

Step 6 **redistribute isis** *instance* [**level-1** | **level-2** | **level-1-2**] [**metric** *metric*] [**metric-type** { **internal** | **external** }] [**policy** *policy-name*]

Example:

```
RP/0/RP0:hostname(config-isis-af)# redistribute isis 2 level-1
```

(Optional) Redistributes routes from one IS-IS instance into another instance.

- In this example, an IS-IS instance redistributes Level 1 routes from another IS-IS instance.

Step 7 Do the following:

- **summary-prefix** *address* / *prefix-length* [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-af)# summary-prefix 10.1.0.0/16 level 1
```

or

```
RP/0/RP0:hostname(config-isis-af)# summary-prefix 3003:xxxx::/24 level 1
```

(Optional) Allows a Level 1-2 router to summarize Level 1 IPv4 prefixe at Level 2, instead of advertising the Level 1 prefixes directly when the router advertises the summary.

- This example specifies an IPv4 address and mask.

Step 8 **maximum-paths** *route-number*

Example:

```
RP/0/RP0:hostname(config-isis-af)# maximum-paths 16
```

(Optional) Configures the maximum number of parallel paths allowed in a routing table.

Step 9 **distance** *weight* [*address / prefix-length* [*route-list-name*]]

Example:

```
RP/0/RP0:hostname(config-isis-af)# distance 90
```

(Optional) Defines the administrative distance assigned to routes discovered by the IS-IS protocol.

- A different administrative distance may be applied for IPv4.

Step 10 **set-attached-bit**

Example:

```
RP/0/RP0:hostname(config-isis-af)# set-attached-bit
```

(Optional) Configures an IS-IS instance with an attached bit in the Level 1 LSP.

Step 11 **commit**

Tagging IS-IS Interface Routes

This optional task describes how to associate a tag with a connected route of an IS-IS interface.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing process, and places the router in router configuration mode. In this example, the IS-IS instance is called isp.

Step 3 **address-family** { **ipv4** } [**unicast**]

Example:

```
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
```

Specifies the IPv4 address family, and enters router address family configuration mode.

Step 4 **metric-style wide** [**transition**] [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-af)# metric-style wide level 1
```

Configures a router to generate and accept only wide link metrics in the Level 1 area.

Step 5 **exit**

Example:

```
RP/0/RP0:hostname(config-isis-af)# exit
```

Exits router address family configuration mode, and returns the router to router configuration mode.

Step 6 **interface** *type number*

Example:

```
RP/0/RP0:hostname(config-isis)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode.

Step 7 **address-family** { **ipv4** } [**unicast**]

Example:

```
RP/0/RP0:hostname(config-isis-if)# address-family ipv4 unicast
```

Specifies the IPv4 address family, and enters address family configuration mode.

Step 8 **tag** *tag*

Example:

```
RP/0/RP0:hostname(config-isis-if-af)# tag 3
```

Sets the value of the tag to associate with the advertised connected route.

Step 9 **commit**

Step 10 **show isis** [**ipv4** | **afi-all**] [**unicast** | **safi-all**] **route** [**detail**]

Example:

```
RP/0/RP0:hostname(config-isis-if-af)# show isis ipv4 route detail
```

Displays tag information. Verify that all tags are present in the RIB.

Setting the Priority for Adding Prefixes to the RIB

This optional task describes how to set the priority (order) for which specified prefixes are added to the RIB. The prefixes can be chosen using an access list (ACL), prefix list, or by matching a tag value.

Procedure

Step 1 **configure**

Step 2 **router isis** *instance-id*

Example:

```
RP/0/RP0:hostname(config)# router isis isp
```

Enables IS-IS routing for the specified routing process, and places the router in router configuration mode. In this example, the IS-IS instance is called isp.

Step 3 **address-family** { **ipv4** } [**unicast**]

Example:

```
RP/0/RP0:hostname(config-isis)# address-family ipv4 unicast
```

Specifies the IPv4 address family, and enters router address family configuration mode.

Step 4 **metric-style wide** [**transition**] [**level** { **1** | **2** }]

Example:

```
RP/0/RP0:hostname(config-isis-af)# metric-style wide level 1
```

Configures a router to generate and accept only wide-link metrics in the Level 1 area.

Step 5 **spf prefix-priority** [**level** { **1** | **2** }] { **critical** | **high** | **medium** } { *access-list-name* | **tag** *tag* }

Example:

```
RP/0/RP0:hostname(config-isis-af)# spf prefix-priority high tag 3
```

Installs all routes tagged with the value 3 first.

Step 6 **commit**

Configuration Examples for Implementing IS-IS

This section provides the following configuration examples:

Redistributing IS-IS Routes Between Multiple Instances: Example

The following example shows usage of the **set- attached-bit** and **redistribute** commands. Two instances, instance “1” restricted to Level 1 and instance “2” restricted to Level 2, are configured.

The Level 1 instance is propagating routes to the Level 2 instance using redistribution. Note that the administrative distance is explicitly configured higher on the Level 2 instance to ensure that Level 1 routes are preferred.

Attached bit is being set for the Level 1 instance since it is redistributing routes into the Level 2 instance. Therefore, instance “1” is a suitable candidate to get from the area to the backbone.

```
  router isis 1
    is-type level-2-only
   net 49.0001.0001.0001.0001.00
   address-family ipv4 unicast
    distance 116
    redistribute isis 2 level 2
  !
  interface TenGigE 0/3/0/0
   address-family ipv4 unicast
  !
  !
  router isis 2
   is-type level-1
   net 49.0002.0001.0001.0002.00
   address-family ipv4 unicast
    set
-attached
  !
  interface TenGigE 0/1/0/0
   address-family ipv4 unicast
```

Configuring IS-IS Overload Bit Avoidance: Example

The following example shows how to activate IS-IS overload bit avoidance:

```
RP/0/RP0:hostname# config
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# config
RP/0/RP0:hostname(config)# no mpls traffic-eng path-selection ignore overload
```

Tagging Routes: Example

The following example shows how to tag routes.

```
route-policy isis-tag-55
end-policy
!
route-policy isis-tag-555
  if destination in (5.5.5.0/24 eq 24) then
    set tag 555
    pass
  else
    drop
  endif
end-policy
!
router static
 address-family ipv4 unicast
  0.0.0.0/0 2.6.0.1
  5.5.5.0/24 Null0
 !
!
router isis uut
```

```
  net 00.0000.0000.12a5.00
  address-family ipv4 unicast
   metric-style wide
   redistribute static level-1 route-policy isis-tag-555
   spf prefix-priority critical tag 13
   spf prefix-priority high tag 444
   spf prefix-priority medium tag 777
```

Configuring IS-IS Overload Bit Avoidance: Example

The following example shows how to activate IS-IS overload bit avoidance:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# mpls traffic-eng path-selection ignore overload
```

The following example shows how to deactivate IS-IS overload bit avoidance:

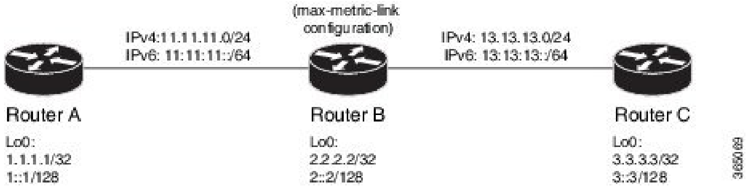
```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# no mpls traffic-eng path-selection ignore overload
```

Example: Configuring IS-IS To Handle Router Overload

This section describes an example for configuring IS-IS to handle overloading of routers, without setting the overload bit.

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). To configure the overload behavior for IS-IS, without setting the overload bit, configure the **max-link-metric** statement. By configuring this statement, the router participates in the routing process and is used as a transit node of last resort.

Figure 8:



Before you begin

Ensure that you are familiar with configuring router interfaces for a given topology.

Procedure

Step 1 Configure Routers A, B, and C as shown in the topology.

Use the following IP Addresses:

- **Router A Loopback0**: 1.1.1.1/32 and 1::1/128

- **Router A -> Router B**: 11.11.11.2/24 and 11:11:11::2/64
- **Router B Loopback0**: 2.2.2.2/32 and 2::2/128
- **Router B -> Router A**: 11.11.11.1/24 and 11:11:11::1/64
- **Router B-> Router C**: 13.13.13.1/24 and 13:13:13::1/64
- **Router C Loopback0**: 3.3.3.3/32 and 3::3/128
- **Router C-> Router B**: 13.13.13.2/24 and 13:13:13::2/64

Step 2 Configure IS-IS and the corresponding net addresses on Routers A, B and C.

Example:

```
!Router A
RP/0/RP0::RouterA(config)# router isis ring
RP/0/RP0::RouterA(config-isis)# net 00.0000.0000.0001.00
RP/0/RP0:RouterA(config-isis)# address-family ipv4 unicast
RP/0/RP0:RouterA(config-isis)# metric-style wide
RP/0/RP0:RouterA(config-isis-af)# exit

!Router B
RP/0/RP0:RouterB(config)# router isis ring
RP/0/RP0:RouterB(config-isis)# net 00.0000.0000.0002.00
RP/0/RP0:RouterB(config-isis)# address-family ipv4 unicast
RP/0/RP0:RouterB(config-isis-af)# exit

!Router C
RP/0/RP0:RouterC(config)# router isis ring
RP/0/RP0:RouterC(config-isis)# net 00.0000.0000.0003.00
RP/0/RP0:RouterC(config-isis)# address-family ipv4 unicast
RP/0/RP0:RouterA(config-isis)# metric-style wide
RP/0/RP0:RouterC(config-isis-af)# exit
```

Step 3 Configure IPv4 address families on the loopback interfaces of Routers A, B, and C.

Example:

```
RP/0/RP0:Router(config-isis)# interface loopback0
RP/0/RP0:Router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:Router(config-isis-if-af)# exit
RP/0/RP0:Router(config-isis-if)# exit
RP/0/RP0:Router(config-isis)#
```

Step 4 Configure the link metrics on the router interfaces.

Example:

```
! Configuration for Router A Interface TenGigE 0/0/0/0 with Router B is shown here. Similarly,
 configure other router interfaces.
RP/0/RP0:RouterA(config-isis)# interface TenGigE 0/0/0/0
RP/0/RP0:RouterA(config-isis-if)# address-family ipv4 unicast
RP/0/RP0:RouterA(config-isis-if-af)# metric 10
RP/0/RP0:RouterA(config-isis-if-af)# exit
RP/0/RP0:RouterA(config-isis-if)# exit
RP/0/RP0:RouterA(config-isis)#
```

Step 5 Confirm your configuration by viewing the route prefixes on Routers A, B, and C.

Example:

```
! The outputs for Router A are shown here. Similarly, view the outputs for Routers B and
```

```
C.
RP/0/RP0:RouterA# show route
Tue Oct 13 13:55:18.342 PST

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
       A - access/subscriber, a - Application route
       M - mobile route, (!) - FRR Backup path

Gateway of last resort is not set

L    1.1.1.1/32 is directly connected, 00:03:40, Loopback0
i L1 2.2.2.2/32 [115/20] via 11.11.11.2, 00:01:27, TenGigE0/0/0/0
i L1 3.3.3.3/32 [115/30] via 11.11.11.2, 00:01:27, TenGigE0/0/0/0
C    11.11.11.0/24 is directly connected, 00:03:39, TenGigE0/0/0/0
L    11.11.11.1/32 is directly connected, 00:03:39, TenGigE0/0/0/0
i L1 13.13.13.0/24 [115/20] via 11.11.11.2, 00:01:27, TenGigE0/0/0/0
i L1 15.15.15.0/24 [115/30] via 11.11.11.2, 00:01:27, TenGigE0/0/0/0
```

Step 6 Confirm the link metrics on Router B, prior to configuring the **max-link-metric** statement.

Example:

```
RP/0/RP0:RouterB# show isis database
Tue Oct 13 13:56:44.077 PST

No IS-IS RING levels found
IS-IS ring (Level-1) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
RouterB.00-00           * 0x00000005   0x160d        1026            0/0/0
  Area Address: 00
  NLPID:        0xcc
  NLPID:        0x8e
  MT:           Standard (IPv4 Unicast)
  Hostname:     RouterB
  IP Address:   2.2.2.2


  Metric: 10         IS RouterB.01
  Metric: 10         IS RouterA.00
  Metric: 10         IP 2.2.2.2/32
  Metric: 10         IP 11.11.11.0/24
  Metric: 10         IP 13.13.13.0/24
  Metric: 10         MT (IPv4 Unicast) IS-Extended RouterB.01
  Metric: 10         MT (IPv4 Unicast) IS-Extended RouterA.00
  Metric: 10         MT (IPv4 Unicast) IPv4 2::2/128
  Metric: 10         MT (IPv4 Unicast) IPv4 11:11:11::/64
  Metric: 10         MT (IPv4 Unicast) IPv4 13:13:13::/64
RouterB.01-00             0x00000001   0xc8df        913             0/0/0
  Metric: 0          IS RouterB.00
  Metric: 0          IS RouterC.00
  Metric: 0          IS-Extended RouterB.00
  Metric: 0          IS-Extended RouterC.00

 Total Level-1 LSP count: 2     Local Level-1 LSP count: 1
```

The output verifies that IS-IS protocol is operational and the displayed link metrics (**Metric: 10**) are as configured.

Step 7 Configure the **max-link-metric** statement on Router B.

Example:

```
RP/0/RP0:RouterB(config)# router isis ring
RP/0/RP0:RouterB(config-isis)# max-link-metric
RP/0/RP0:RouterB(config-isis)# exit
RP/0/RP0:RouterB(config)#
```

Step 8 Commit your configuration.

Example:

```
RP/0/RP0:RouterB(config)# commit
```

Step 9 Confirm the change in link metrics on Router B.

Example:

```
RP/0/RP0:RouterB# show isis database
Tue Oct 13 13:58:36.790 PST

No IS-IS RING levels found
IS-IS ring (Level-1) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
RouterB.00-00           * 0x00000006   0x0847        1171            0/0/0
  Area Address: 00
  NLPID:        0xcc
  NLPID:        0x8e
  MT:           Standard (IPv4 Unicast)
  MT:           IPv4 Unicast                                    0/0/0
  Hostname:     RouterB
  IP Address:   2.2.2.2
  IPv4 Address: 2::2
  Metric: 63         IS RouterB.01
  Metric: 63         IS RouterA.00
  Metric: 63         IP 2.2.2.2/32
  Metric: 63         IP 11.11.11.0/24
  Metric: 63         IP 13.13.13.0/24
  Metric: 16777214   MT (IPv4 Unicast) IS-Extended RouterB.01
  Metric: 16777214   MT (IPv4 Unicast) IS-Extended RouterA.00
  Metric: 16777214   MT (IPv4 Unicast) IPv4 2::2/128
  Metric: 16777214   MT (IPv4 Unicast) IPv4 11:11:11::/64
  Metric: 16777214   MT (IPv4 Unicast) IPv4 13:13:13::/64
RouterB.01-00             0x00000001   0xc8df        800             0/0/0
  Metric: 0          IS RouterB.00
  Metric: 0          IS RouterC.00
  Metric: 0          IS-Extended RouterB.00
  Metric: 0          IS-Extended RouterC.00

 Total Level-1 LSP count: 2     Local Level-1 LSP count: 1
```

The output verifies that maximum link metrics (**63** for IPv4 has been allocated for the designated links.

Step 10 (Optional) Verify the change in route prefixes on Routers A and C.

Example:

```
! The outputs for Router A are shown here. Similarly, view the outputs on Router C.
RP/0/RP0:RouterA# show route
Tue Oct 13 13:58:59.289 PST

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
       A - access/subscriber, a - Application route
       M - mobile route, (!) - FRR Backup path

Gateway of last resort is not set

L    1.1.1.1/32 is directly connected, 00:07:21, Loopback0
i L1 2.2.2.2/32 [115/73] via 11.11.11.2, 00:00:50, TenGigE0/0/0/0
i L1 3.3.3.3/32 [115/83] via 11.11.11.2, 00:00:50, TenGigE0/0/0/0
C    11.11.11.0/24 is directly connected, 00:07:20, TenGigE0/0/0/0
L    11.11.11.1/32 is directly connected, 00:07:20, TenGigE0/0/0/0
i L1 13.13.13.0/24 [115/73] via 11.11.11.2, 00:00:50, TenGigE0/0/0/0
i L1 15.15.15.0/24 [115/83] via 11.11.11.2, 00:00:50, TenGigE0/0/0/0
```

The output verifies the impact of maximum metric configuration in the routing table: **[115/73]** and **[115/83]**

IS-IS has been successfully configured to handle router overload without setting the overload bit.

CHAPTER 37

Bidirectional Forwarding Detection

This chapter includes details for Bidirectional Forwarding Detection (BFD).

BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators.

Bidirectional Forwarding Detection

Bidirectional forwarding detection (BFD) provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines. BFD allows a single mechanism to be used for failure detection over any media and at any protocol layer, with a wide range of detection times and overhead. The fast detection of failures provides immediate reaction to failure in the event of a failed link or neighbor.

Prerequisites for Implementing BFD

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 following prerequisites are required to implement BFD:

- Interior Gateway Protocol (IGP) is activated on the router if you are using IS-IS or OSPF.
- To enable BFD for a neighbor, the neighbor router must support BFD.

Restrictions for Implementing BFD

These restrictions apply to BFD:

- Demand mode is not supported.
- Asynchronous echo mode is not supported.

- Mutli hop BFD is not supported.
- BFD for bundles is not supported.

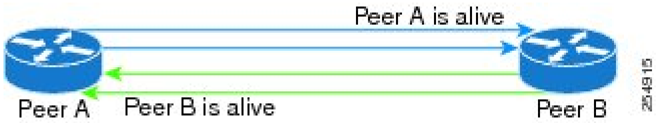
Operating Modes for BFD

BFD can operate in two modes, Asynchronous mode and Demand mode. Cisco NCS 4000 supports the asynchronous mode only. In this mode, the systems periodically send BFD control packets to one another. If a number of those packets in a row, are not received by the other system, the session is declared to be down.

When BFD is running asynchronously, the following happens:

- Each system periodically sends BFD control packets to one another. Packets sent by BFD router “Peer A” to BFD router “Peer B” have a source address from Peer A and a destination address for Peer B.
- Control packet streams are independent of each other and do not work in a request/response model.
- If a number of packets in a row are not received by the other system, the session is declared down.

Figure 9: BFD Asynchronous Mode



Control packet failure in asynchronous mode (without echo), is detected using the values of the minimum interval (**bfd minimum-interval**) and multiplier (**bfd multiplier**) commands. For control packet failure detection, the local multiplier value is sent to the neighbor. A failure detection timer is started based on (*I x M*), where *I* is the negotiated interval, and *M* is the multiplier provided by the remote end. Whenever a valid control packet is received from the neighbor, the failure detection timer is reset. If a valid control packet is not received from the neighbor within the time period (*I x M*), then the failure detection timer is triggered, and the neighbor is declared down.

Table 34: BFD Packet Intervals

Configured Async Control Packet Interval (ms)	Multiplier value (the default is 3; range is from 2 to 50)	Async Control Packet Failure Detection Time (ms) (Interval X Multiplier) The multiplier value is set to the default value of 3
3.3 (rounded off to 3)	3	9
10	3	30
20	3	60
50	3	150
100	3	300
1000	3	3000

Configured Async Control Packet Interval (ms)	Multiplier value (the default is 3; range is from 2 to 50)	Async Control Packet Failure Detection Time (ms) (Interval X Multiplier) The multiplier value is set to the default value of 3
2000 (this value is the default value)	3	6000

BFD for IPv4

Cisco NCS 4000 supports single hop BFD for IPv4.

BFD asynchronous packets are transmitted over UDP and IPv4 using source port 49152 and destination port 3784. For asynchronous mode, the source address of the IP packet is the local interface address, and the destination address is the remote interface address.

BFD is supported for connections over the following interface types:

- Gigabit Ethernet (GigE)
- Ten Gigabit Ethernet (10GigE)
- Hundred Gigabit Ethernet (100GigE)

BFD Dampening

Bidirectional Forwarding Detection (BFD) is a mechanism used by routing protocols to quickly realize and communicate the reachability failures to their neighbors. When BFD detects a reachability status change of a client, its neighbors are notified immediately. Sometimes it might be critical to minimize changes in routing tables so as not to impact convergence, in case of a micro failure. An unstable link that flaps excessively can cause other devices in the network to consume substantial processing resources, and that can cause routing protocols to lose synchronization with the state of the flapping link.

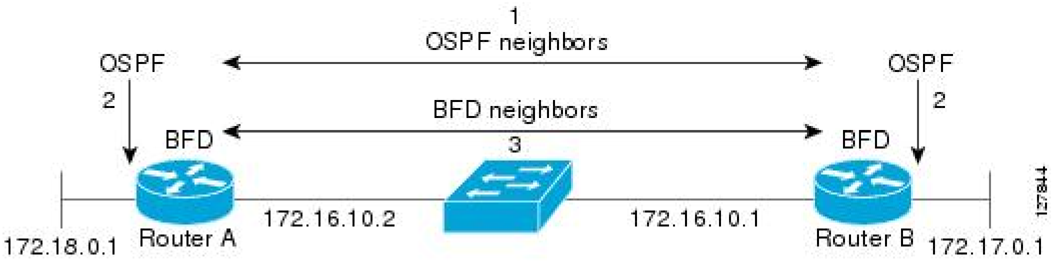
The BFD dampening feature introduces a configurable exponential delay mechanism. This mechanism is designed to suppress the excessive effect of remote node reachability events flapping with BFD. The BFD Dampening feature allows the network operator to automatically dampen a given BFD session to prevent excessive notification to BFD clients, thus preventing unnecessary instability in the network. Dampening the notification to a BFD client suppresses BFD notification until the time the session under monitoring stops flapping and becomes stable.

Implementing BFD

By sending rapid failure detection notices to the routing protocols in the local router to initiate the routing table recalculation process, BFD contributes to greatly reduced overall network convergence time.

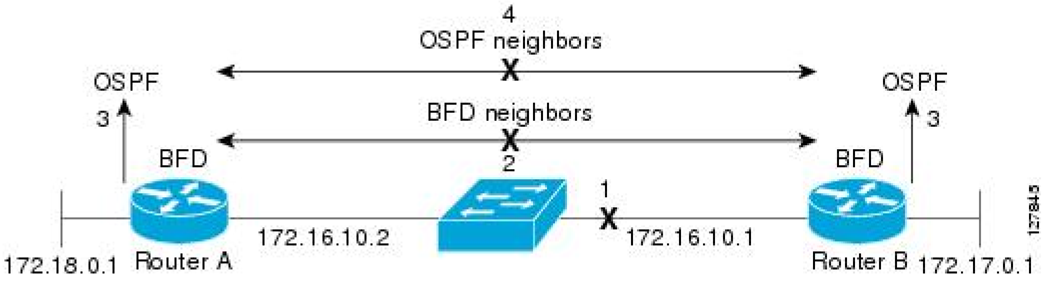
The figure below, shows a simple network with two routers running OSPF and BFD. When OSPF discovers a neighbor (1) it sends a request to the local BFD process to initiate a BFD neighbor session with the OSPF neighbor router (2). The BFD neighbor session with the OSPF neighbor router is established (3).

Figure 10: BFD process - establishing a connection



The figure below, shows what happens when a failure occurs on the network (1). The BFD neighbor session with the OSPF neighbor router is not reachable (2). BFD notifies the local OSPF process that the BFD neighbor is no longer reachable (3). The local OSPF process deletes the OSPF neighbor relationship (4). If an alternative path is available the routers will immediately start converging on it.

Figure 11: BFD process - failure detection



BFD over Bundle

Table 35: Feature History

Feature Name	Release Information	Feature Description
Bidirectional Forwarding Detection (BFD) over Link Aggregation Group (LAG)	Cisco IOS XR Release 6.5.31	BFD allows you to detect network failures between neighbors. Two modes are supported: • BFD over Bundle (BoB) - Standards-based fast failure detection of non-VLAN interfaces in LAG. • BFD over Logical Bundle - Standards-based fast failure detection of VLAN interfaces in LAG. Commands added: • interface Bundle-Ether • bfd address-family • bfd mode • bundle minimum-active • encapsulation dot1q • bfd fast-detect • bfd minimum-interval • bfd multiplier

BFD over Bundle (BoB) mode is a standard based fast failure detection of Link Aggregation Group (LAG) member links. BoB supports only IETF standard for each bundle.

Note The BFD client is bundlemgr for BFD over Bundle. Hence if BFD session goes down, bundlemgr brings down the bundle, and this in turn brings down the routing session.

Restrictions

- To support BFD on bundle member links, ensure that the routers on either end of the bundle are connected back-to-back without a Layer 2 switch in between.
- Do not configure the BoB and BFD over Logical Bundle (BLB) features simultaneously on the same bundle.

Configuring BoB

Configuring BoB involves configuring the following tasks:

- Enabling BFD Sessions on Bundle Members, on page 398
- Specifying the BFD Destination Address on a Bundle, on page 398
- Configuring the Minimum Thresholds to Maintain an Active Bundle, on page 399
- Configuring BFD Packet Transmission Intervals and Failure Detection Times on a Bundle, on page 400
- Enabling IETF Mode for BFD over Bundle, on page 401

Enabling BFD Sessions on Bundle Members

This procedure describes how to enable BFD sessions on bundle member links.

Procedure

Step 1 **configure**

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
```

Enters interface configuration mode for the specified bundle ID.

Step 3 **bfd address-family ipv4 fast-detect**

Example:

```
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 fast-detect
```

Enables IPv4 BFD sessions on bundle member links.

Step 4 **bfd mode ietf**

Example:

```
RP/0/RP0:hostname(config-if)# bfd mode ietf
```

Enables IETF mode for BFD over bundle for the specified bundle.

Step 5 **commit**

Specifying the BFD Destination Address on a Bundle

This procedure describes how to specify the BFD destination address on a bundle.

Procedure

Step 1 **configure**

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
```

Enters interface configuration mode for the specified bundle ID.

Step 3 **bfd address-family ipv4 destination** *ip-address*

Example:

```
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 destination 10.20.20.1
```

Specifies the primary IPv4 address assigned to the bundle interface on a connected remote system, where *ip-address* is the 32-bit IP address in dotted-decimal format (A.B.C.D).

Step 4 **commit**

Configuring the Minimum Thresholds to Maintain an Active Bundle

The bundle manager uses two configurable minimum thresholds to determine whether a bundle can be brought up or remain up, or is down, based on the state of its member links.

- Minimum active number of links
- Minimum active bandwidth available

Whenever the state of a member changes, the bundle manager determines whether the number of active members or available bandwidth is less than the minimum. If so, then the bundle is placed, or remains, in DOWN state. Once the number of active links or available bandwidth reaches one of the minimum thresholds, then the bundle returns to the UP state.

This procedure describes how to configure minimum bundle thresholds.

Procedure

Step 1 **configure**

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
```

Enters interface configuration mode for the specified bundle ID.

Step 3 **bundle minimum-active bandwidth** *kbps*

Example:

```
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 580000
```

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.

Step 4 **bundle minimum-active links** *links*

Example:

```
RP/0/RP0:hostname(config-if)# bundle minimum-active links 2
```

Sets the number of active links required before a bundle can be brought up or remain up. The range is from 1 to 16.

Step 5 **commit**

Configuring BFD Packet Transmission Intervals and Failure Detection Times on a Bundle

BFD asynchronous packet intervals and failure detection times for BFD sessions on bundle member links are configured using a combination of the **bfd address-family ipv4 minimum-interval** and **bfd address-family ipv4 multiplier** interface configuration commands on a bundle.

BFD asynchronous packet intervals and failure detection times for BFD sessions on bundle member links are configured using a combination of the **bfd address-family ipv4 minimum-interval** and **bfd address-family ipv4 multiplier** interface configuration commands on a bundle.

This procedure describes how to configure the minimum transmission interval and failure detection times for BFD asynchronous mode control packets on bundle member links.

Procedure

Step 1 **configure**

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
```

Enters interface configuration mode for the specified bundle ID.

Step 3 **bfd address-family ipv4 minimum-interval** *milliseconds*

Example:

```
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 minimum-interval 2000
```

Specifies the minimum interval, in milliseconds, for asynchronous mode control packets on IPv4 BFD sessions on bundle member links. The range is from 4 to 30000.

Step 4 **bfd address-family ipv4 multiplier** *multiplier*

Example:

```
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 multiplier 3
```

Specifies 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. We recommend to have multiplier value of 3.

Step 5 **commit**

Enabling IETF Mode for BFD over Bundle

This procedure describes how to enable IETF mode for BFD over bundle.

Procedure

Step 1 **configure**

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
```

Enters interface configuration mode for the specified bundle ID.

Step 3 **bfd mode ietf**

Example:

```
RP/0/RP0:hostname(config-if)# bfd mode ietf
```

Enables IETF mode for BFD over bundle for the specified bundle.

Step 4 **bfd address-family ipv4 fast-detect**

Example:

```
RP/0/RP0:hostname(config-if)# bfd address-family ipv4 fast-detect
```

Enables IPv4 BFD sessions on the specified bundle.

Step 5 **commit**

Running Configuration

This section shows a sample of BFD over bundle configuration.

R1:

```
interface FortyGigE0/2/0/2
bundle id 1 mode active
!

interface bundle-ether1
ipv4 address 172.31.13.6 255.255.255.252
bfd address-family ipv4 multiplier 3
bfd address-family ipv4 destination 172.31.13.5
bfd address-family ipv4 fast-detect
bfd address-family ipv4 minimum-interval 200
!
```

R2:

```
interface FortyGigE0/2/0/2
bundle id 1 mode active

interface Bundle-Ether1
ipv4 address 172.31.13.5 255.255.255.252
bfd address-family ipv4 multiplier 3
bfd address-family ipv4 destination 172.31.13.6
bfd address-family ipv4 fast-detect
bfd address-family ipv4 minimum-interval 200
```

BFD over Logical Bundle

Bidirectional Forwarding Detection (BFD) over Logical Bundle (BLB) feature implements and deploys BFD over bundle VLAN interfaces.

BLB feature is different from the BFD over Bundle (BoB) feature which runs on non-VLAN bundle interfaces. These two features are distinct from each other. Do not configure these two features simultaneously on the same bundle.

Note Routing protocols are BFD clients for the BLB feature. Hence if BFD session goes down, it will bring down the routing session. The default timer is 50 milliseconds.

Restrictions

- BLB sessions are restricted to an interval of 300 milliseconds and a multiplier of 3. Though you can configure more aggressive parameters, Cisco does not recommend it.
- Do not configure the BLB and BFD over Bundle (BoB) features simultaneously on the same bundle.

Configuring BLB

Configuring BLB involves configuring the following tasks:

- Creating VLAN Sub-interface under Bundle Interface
- Enable BFD for OSPF on an Interface
- Configuring a Line Card to Host BLB Sessions

Creating VLAN Sub-interface under Bundle Interface

This procedure describes how to create VLAN sub-interface under the bundle interface.

Procedure

Step 1 **configure**

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
```

Enters interface configuration mode for the specified bundle ID.

Step 3 **ipv4 address** *ip-address subnet-mask*

Example:

```
RP/0/RP0:hostname(config-if)# ipv4 address 10.1.1.1 255.255.255.0
```

Specifies IP address and subnet mask.

Step 4 **encapsulation dot1q** *vlan-id*

Example:

```
RP/0/RP0:hostname(config-if)# encapsulation dot1q 1
```

Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

Step 5 **commit**

Enable BFD for OSPF on an Interface

This procedure describes how to enable BFD for Open Shortest Path First (OSPF) on an interface. The steps in this procedure are applicable to IS-IS as well. In case of IS-IS, the command mode is different.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

```
RP/0/RP0:hostname(config)# router ospf 10
```

Enters the OSPF configuration mode. For the IS-IS routing protocol, use the **router isis** command.

Step 3 **area** *area-id*

Example:

```
RP/0/RP0:hostname(config)# area 10
```

Configures an OSPF area . This command is not applicable to IS-IS.

Step 4 **interface** *type location*

Example:

```
RP/0/RP0:hostname(config-ospf)# interface Bundle-Ether 1
```

Enters the interface configuration mode and specifies the interface for BFD configuration.

Step 5 **bfd fast-detect**

Example:

```
RP/0/RP0:hostname(config-ospf-if)# bfd fast-detect
```

Enables BFD to detect failures in the path between adjacent forwarding engines. For IS-IS, use the **bfd fast-detect ipv4** command.

Step 6 **bfd minimum-interval** *milliseconds*

Example:

```
RP/0/RP0:hostname(config-ospf-if)# bfd minimum-interval 100
```

Sets the minimum control packet interval for the BFD sessions. The supported BFD minimum-interval timer value is 100 ms.

Step 7 **bfd multiplier** *value*

Example:

```
RP/0/RP0:hostname(config-ospf-if)# bfd multiplier 3
```

Sets the BFD multipler value. The default value is 3. We recommend to have a multiplier value of 3.

Step 8 **commit**

Enabling BFD on a BGP Neighbor

This procedure describes how to enable BFD on a BGP per neighbor, or per interface.

Table 36: Feature History

Feature Name	Release Information	Description
BFD on BGP	Cisco IOS XR Release 6.5.33	Bidirectional Forwarding Detection (BFD) is now enabled on the Broad Gateway Protocol (BGP). BFD provides a single, standardized link/device/protocol failure detection method at any protocol layer and over any media. This feature offers quick failure detection between BGP nodes, allowing faster traffic rerouting to an alternate path.

Note BFD neighbor router configuration is available for BGP only.

Note BFD strict mode is not supported.

Procedure

Step 1 **configure**

Step 2 **router bgp** *autonomous-system-number*

Example:

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

Enters BGP configuration mode, allowing you to configure the BGP routing process, use the **show bgp command** in EXEC mode to obtain the *autonomous-system-number* for the current router.

Step 3 **neighbor** *ip-address*

Example:

```
RP/0/RP0:hostname(config-bgp)#neighbor 192.0.2.2
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.

This example configures the IP address 192.0.2.2 as a BGP peer.

Step 4 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)#remote-as 1
```

Creates a neighbor and assigns it a remote autonomous system.

This example configures the remote autonomous system to be 1.

Step 5 **bfd multiplier** *multiplier*

Example:

```
RP/0/RP0:hostname(config-bgp)#bfd multipier 3
```

Sets the BFD multiplier.

Step 6 **bfd minimum-interval** *milliseconds*

Example:

```
RP/0/RP0:hostname(config-bgp)#bfd minimum-interval 20
```

Sets the BFD minimum interval. Range is 4-30000 milliseconds.

Step 7 **bfd fast-detect** *autonomous-system-number*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)#bfd fast-detect
```

Enables BFD between the local networking devices and the neighbor whose IP address you configured to be a BGP peer in step 3.

In Step 3, the IP address 192.0.2.2 was configured as the BGP peer. In this example, BFD is enabled between the local networking devices and the neighbor 192.0.2.2.

Step 8 **update-source** *interface-type interface-number*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)#update-source hundredgige0/4/0/5.1
```

It checks routing sources to ensure that the incoming routing update's source IP address is on the same network as the interface receiving the update.

Step 9 **address-family ipv4** [**unicast|multicast**]

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)#address-family ipv4 labeled unicast
```

The **address-family ipv4** declares neighbors with whom you want to exchange normal "IPv4 unicast" routes.

Step 10 **route-reflector-client**

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)#route-reflector-client
```

It provides the unique BGP capability of republishing routes learned from an internal peer to other internal peers.

Step 11 **next-hop-self**

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)#next-hop-self
```

It disables the next hop calculation for this neighbor.

Step 12 **commit**

Saves the configuration changes and remains within the configuration session.

Configuring a Line Card to Host BLB Sessions

The BLB sessions and bundle member links need not be configured on the same line card.

Procedure

Step 1 **configure**

Step 2 **bfd**

Example:

```
RP/0/RP0:hostname(config)# bfd
```

Enters BFD configuration mode.

Step 3 **multipath include location** *location*

Example:

```
RP/0/RP0:hostname(config-bfd)# multipath include location 0/2/CPU0
```

Defines the line card to host BLB and BFD multihop sessions.

Step 4 **commit**

Running Configuration

This section shows a sample of BFD over logical bundle configuration.

R1:

```
interface GigabitEthernet0/1/0/6
bundle id 200 mode active

interface GigabitEthernet0/1/0/7
bundle id 200 mode active

interface GigabitEthernet0/1/0/8
bundle id 200 mode active

interface Bundle-Ether200.10
ipv4 address 172.31.13.5 255.255.255.252
encapsulation dot1q 10
!
!

bfd
multipath include location 0/2/CPU0
!

router ospf 100
area 0
  interface Bundle-Ether200.10
    bfd minimum-interval 100
    bfd fast-detect
    bfd multiplier 3
  !
!
!
```

R2:

```
interface GigabitEthernet0/0/0/36
bundle id 200 mode active

interface GigabitEthernet0/0/0/37
bundle id 200 mode active

interface GigabitEthernet0/0/0/39
bundle id 200 mode active

interface Bundle-Ether200.10
ipv4 address 172.31.13.6 255.255.255.252
encapsulation dot1q 10
!

bfd
multipath include location 0/0/CPU0
!
```

```
router ospf 100
area 0
  interface Bundle-Ether200.10
   bfd minimum-interval 100
   bfd fast-detect
   bfd multiplier 3
  !
!
!
```

CHAPTER 38

OSPF-IPv4

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). Designed expressly for IP networks, OSPF supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. This chapter describes the concepts and tasks you need to configure OSPF on your Cisco NCS 4000 Series Router.

Prerequisites for Implementing OSPF

The following are prerequisites for implementing OSPF on Cisco IOS XR software:

- 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.k
- Configuring authentication (IP Security) is an optional task. If you choose to configure authentication, you must first decide whether to configure plain text or Message Digest 5 (MD5) authentication, and whether the authentication applies to an entire area or specific interfaces.

Information About Implementing OSPF

To implement OSPF you need to understand the following concepts:

OSPF Functional Overview

OSPF is a routing protocol for IP. It is a link-state protocol, as opposed to a distance-vector protocol. A link-state protocol makes its routing decisions based on the states of the links that connect source and destination machines. The state of the link is a description of that interface and its relationship to its neighboring networking devices. The interface information includes the IP address of the interface, network mask, type of network to which it is connected, routers connected to that network, and so on. This information is propagated in various types of link-state advertisements (LSAs).

A router stores the collection of received LSA data in a link-state database. This database includes LSA data for the links of the router. The contents of the database, when subjected to the Dijkstra algorithm, extract data to create an OSPF routing table. The difference between the database and the routing table is that the database contains a complete collection of raw data; the routing table contains a list of shortest paths to known destinations through specific router interface ports.

OSPF is the IGP of choice because it scales to large networks. It uses areas to partition the network into more manageable sizes and to introduce hierarchy in the network. A router is attached to one or more areas in a network. All of the networking devices in an area maintain the same complete database information about the link states in their area only. They do not know about all link states in the network. The agreement of the database information among the routers in the area is called convergence.

At the intradomain level, OSPF can import routes learned using Intermediate System-to-Intermediate System (IS-IS). OSPF routes can also be exported into IS-IS. At the interdomain level, OSPF can import routes learned using Border Gateway Protocol (BGP). OSPF routes can be exported into BGP.

Note Following are the number of routes supported in NCS 4000 :

- 32K with NCS4K-2H10T-OP-KS line card
- 32K with NCS4K-4H-OPW-QC2 line card

Unlike Routing Information Protocol (RIP), OSPF does not provide periodic routing updates. On becoming neighbors, OSPF routers establish an adjacency by exchanging and synchronizing their databases. After that, only changed routing information is propagated. Every router in an area advertises the costs and states of its links, sending this information in an LSA. This state information is sent to all OSPF neighbors one hop away. All the OSPF neighbors, in turn, send the state information unchanged. This flooding process continues until all devices in the area have the same link-state database.

To determine the best route to a destination, the software sums all of the costs of the links in a route to a destination. After each router has received routing information from the other networking devices, it runs the shortest path first (SPF) algorithm to calculate the best path to each destination network in the database.

The networking devices running OSPF detect topological changes in the network, flood link-state updates to neighbors, and quickly converge on a new view of the topology. Each OSPF router in the network soon has the same topological view again. OSPF allows multiple equal-cost paths to the same destination. Since all link-state information is flooded and used in the SPF calculation, multiple equal cost paths can be computed and used for routing.

On broadcast and non broadcast multiaccess (NBMA) networks, the designated router (DR) or backup DR performs the LSA flooding. On point-to-point networks, flooding simply exits an interface directly to a neighbor.

OSPF runs directly on top of IP; it does not use TCP or User Datagram Protocol (UDP). OSPF performs its own error correction by means of checksums in its packet header and LSAs.

OSPF typically requires coordination among many internal routers: Area Border Routers (ABRs), which are routers attached to multiple areas, and Autonomous System Border Routers (ASBRs) that export reroutes from other sources (for example, IS-IS, BGP, or static routes) into the OSPF topology. At a minimum, OSPF-based routers or access servers can be configured with all default parameter values, no authentication, and interfaces assigned to areas. If you intend to customize your environment, you must ensure coordinated configurations of all routers.

Key Features Supported in the Cisco IOS XR Software OSPF Implementation

The Cisco IOS XR Software implementation of OSPF conforms to the OSPF Version 2 and OSPF Version 3 specifications detailed in the Internet RFC 2328 and RFC 2740, respectively.

The following key features are supported in the Cisco IOS XR Software implementation:

- Hierarchy—CLI hierarchy is supported.
- Inheritance—CLI inheritance is supported.
- Stub areas—Definition of stub areas is supported.
- NSF—Nonstop forwarding is supported.
- SPF throttling—Shortest path first throttling feature is supported.
- LSA throttling—LSA throttling feature is supported.
- Fast convergence—SPF and LSA throttle timers are set, configuring fast convergence. The OSPF LSA throttling feature provides a dynamic mechanism to slow down LSA updates in OSPF during network instability. LSA throttling also allows faster OSPF convergence by providing LSA rate limiting in milliseconds.
- Route redistribution—Routes learned using any IP routing protocol can be redistributed into any other IP routing protocol.
- Authentication—Plain text and MD5 authentication among neighboring routers within an area is supported.
- Routing interface parameters—Configurable parameters supported include interface output cost, retransmission interval, interface transmit delay, router priority, router “dead” and hello intervals, and authentication key.
- Virtual links—Virtual links are supported.
- Not-so-stubby area (NSSA)—RFC 1587 is supported.
- OSPF over demand circuit—RFC 1793 is supported.

OSPF Hierarchical CLI and CLI Inheritance

Cisco IOS XR Software introduces new OSPF configuration fundamentals consisting of hierarchical CLI and CLI inheritance.

Hierarchical CLI is the grouping of related network component information at defined hierarchical levels such as at the router, area, and interface levels. Hierarchical CLI allows for easier configuration, maintenance, and troubleshooting of OSPF configurations. When configuration commands are displayed together in their hierarchical context, visual inspections are simplified. Hierarchical CLI is intrinsic for CLI inheritance to be supported.

With CLI inheritance support, you need not explicitly configure a parameter for an area or interface. In Cisco IOS XR Software, the parameters of interfaces in the same area can be exclusively configured with a single command, or parameter values can be inherited from a higher hierarchical level—such as from the area configuration level or the router ospf configuration levels.

For example, the hello interval value for an interface is determined by this precedence “IF” statement:

If the **hello interval** command is configured at the interface configuration level, then use the interface configured value, else

If the **hello interval** command is configured at the area configuration level, then use the area configured value, else

If the **hello interval** command is configured at the router ospf configuration level, then use the router ospf configured value, else

Use the default value of the command.

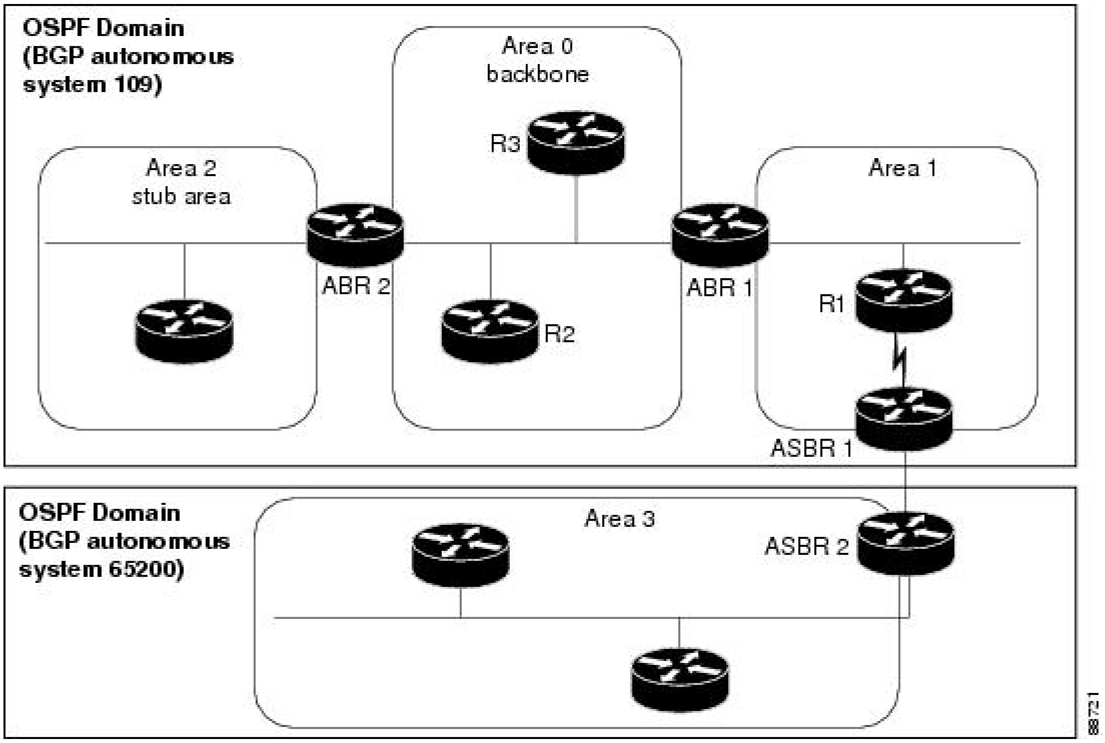
Tip Understanding hierarchical CLI and CLI inheritance saves you considerable configuration time. See Configuring Authentication at Different Hierarchical Levels for OSPF Version 2, on page 439 to understand how to implement these fundamentals. In addition, Cisco IOS XR Software examples are provided in Configuration Examples for Implementing OSPF , on page 471.

OSPF Routing Components

Before implementing OSPF, you must know what the routing components are and what purpose they serve. They consist of the autonomous system, area types, interior routers, ABRs, and ASBRs.

Figure 12: OSPF Routing Components

This figure illustrates the routing components in an OSPF network topology.



Autonomous Systems

The autonomous system is a collection of networks, under the same administrative control, that share routing information with each other. An autonomous system is also referred to as a routing domain. Figure 12: OSPF Routing Components, on page 412 shows two autonomous systems: 109 and 65200. An autonomous system can consist of one or more OSPF areas.

Areas

Areas allow the subdivision of an autonomous system into smaller, more manageable networks or sets of adjacent networks. As shown in Figure 12: OSPF Routing Components, on page 412, autonomous system 109 consists of three areas: Area 0, Area 1, and Area 2.

OSPF hides the topology of an area from the rest of the autonomous system. The network topology for an area is visible only to routers inside that area. When OSPF routing is within an area, it is called *intra-area routing*. This routing limits the amount of link-state information flood into the network, reducing routing traffic. It also reduces the size of the topology information in each router, conserving processing and memory requirements in each router.

Also, the routers within an area cannot see the detailed network topology outside the area. Because of this restricted view of topological information, you can control traffic flow between areas and reduce routing traffic when the entire autonomous system is a single routing domain.

Backbone Area

A backbone area is responsible for distributing routing information between multiple areas of an autonomous system. OSPF routing occurring outside of an area is called *interarea routing*.

The backbone itself has all properties of an area. It consists of ABRs, routers, and networks only on the backbone. As shown in Figure 12: OSPF Routing Components, on page 412, Area 0 is an OSPF backbone area. Any OSPF backbone area has a reserved area ID of 0.0.0.0.

Stub Area

A stub area is an area that does not accept route advertisements or detailed network information external to the area. A stub area typically has only one router that interfaces the area to the rest of the autonomous system. The stub ABR advertises a single default route to external destinations into the stub area. Routers within a stub area use this route for destinations outside the area and the autonomous system. This relationship conserves LSA database space that would otherwise be used to store external LSAs flooded into the area. In Figure 12: OSPF Routing Components, on page 412, Area 2 is a stub area that is reached only through ABR 2. Area 0 cannot be a stub area.

Not-so-Stubby Area

A Not-so-Stubby Area (NSSA) is similar to the stub area. 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.

NSSA allows importing of Type 7 autonomous system external routes within an NSSA area by redistribution. These Type 7 LSAs are translated into Type 5 LSAs by NSSA ABRs, which are flooded throughout the whole routing domain. Summarization and filtering are supported during the translation.

Use NSSA to simplify administration if you are a network administrator that must connect a central site using OSPF to a remote site that is using a different routing protocol.

Before NSSA, the connection between the corporate site border router and remote router could not be run as an OSPF stub area because routes for the remote site could not be redistributed into a stub area, and two routing protocols needed to be maintained. A simple protocol like RIP was usually run and handled the redistribution. With NSSA, you can extend OSPF to cover the remote connection by defining the area between the corporate router and remote router as an NSSA. Area 0 cannot be an NSSA.

Routers

The OSPF network is composed of ABRs, ASBRs, and interior routers.

Area Border Routers

An area border routers (ABR) is a router with multiple interfaces that connect directly to networks in two or more areas. An ABR runs a separate copy of the OSPF algorithm and maintains separate routing data for each area that is attached to, including the backbone area. ABRs also send configuration summaries for their attached areas to the backbone area, which then distributes this information to other OSPF areas in the autonomous system. In Figure 12: OSPF Routing Components, on page 412, there are two ABRs. ABR 1 interfaces Area 1 to the backbone area. ABR 2 interfaces the backbone Area 0 to Area 2, a stub area.

Autonomous System Boundary Routers (ASBR)

An autonomous system boundary router (ASBR) provides connectivity from one autonomous system to another system. ASBRs exchange their autonomous system routing information with boundary routers in other autonomous systems. Every router inside an autonomous system knows how to reach the boundary routers for its autonomous system.

ASBRs can import external routing information from other protocols like BGP and redistribute them as AS-external (ASE) Type 5 LSAs to the OSPF network. If the Cisco IOS XR router is an ASBR, you can configure it to advertise VIP addresses for content as autonomous system external routes. In this way, ASBRs flood information about external networks to routers within the OSPF network.

ASBR routes can be advertised as a Type 1 or Type 2 ASE. The difference between Type 1 and Type 2 is how the cost is calculated. For a Type 2 ASE, only the external cost (metric) is considered when multiple paths to the same destination are compared. For a Type 1 ASE, the combination of the external cost and cost to reach the ASBR is used. Type 2 external cost is the default and is always more costly than an OSPF route and used only if no OSPF route exists.

Interior Routers

An interior router (such as R1 in Figure 12: OSPF Routing Components, on page 412) is attached to one area (for example, all the interfaces reside in the same area).

OSPF Process and Router ID

An OSPF process is a logical routing entity running OSPF in a physical router. This logical routing entity should not be confused with the logical routing feature that allows a system administrator (known as the Cisco IOS XR Software Owner) to partition the physical box into separate routers.

A physical router can run multiple OSPF processes, although the only reason to do so would be to connect two or more OSPF domains. Each process has its own link-state database. The routes in the routing table are calculated from the link-state database. One OSPF process does not share routes with another OSPF process unless the routes are redistributed.

Each OSPF process is identified by a router ID. The router ID must be unique across the entire routing domain. OSPF obtains a router ID from the following sources, in order of decreasing preference:

- By default, when the OSPF process initializes, it checks if there is a router-id in the checkpointing database.
- 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.)
- The ITAL selected router-id.
- The primary IPv4 address of an interface over which this OSPF process is running. The first interface address in the OSPF interface is selected.

We recommend that the router ID be set by the **router-id** command in router configuration mode. Separate OSPF processes could share the same router ID, in which case they cannot reside in the same OSPF routing domain.

Supported OSPF Network Types

OSPF classifies different media into the following types of networks:

- NBMA networks
- Point-to-point networks (POS)
- Broadcast networks (Ten Gigabit Ethernet and Hundred Gigabit Ethernet)
- Point-to-multipoint

You can configure your Cisco IOS XR network as either a broadcast or an NBMA network.

Route Authentication Methods for OSPF

OSPF Version 2 supports two types of authentication: plain text authentication and MD5 authentication. By default, no authentication is enabled (referred to as null authentication in RFC 2178).

OSPV Version 3 supports all types of authentication except key rollover.

Plain Text Authentication

Plain text authentication (also known as Type 1 authentication) uses a password that travels on the physical medium and is easily visible to someone that does not have access permission and could use the password to infiltrate a network. Therefore, plain text authentication does not provide security. It might protect against a faulty implementation of OSPF or a misconfigured OSPF interface trying to send erroneous OSPF packets.

MD5 Authentication

MD5 authentication provides a means of security. No password travels on the physical medium. Instead, the router uses MD5 to produce a message digest of the OSPF packet plus the key, which is sent on the physical medium. Using MD5 authentication prevents a router from accepting unauthorized or deliberately malicious routing updates, which could compromise your network security by diverting your traffic.

Note MD5 authentication supports multiple keys, requiring that a key number be associated with a key.

See OSPF Authentication Message Digest Management, on page 430.

Authentication Strategies

Authentication can be specified for an entire process or area, or on an interface or a virtual link. An interface or virtual link can be configured for only one type of authentication, not both. Authentication configured for an interface or virtual link overrides authentication configured for the area or process.

If you intend for all interfaces in an area to use the same type of authentication, you can configure fewer commands if you use the **authentication** command in the area configuration submode (and specify the **message-digest** keyword if you want the entire area to use MD5 authentication). This strategy requires fewer commands than specifying authentication for each interface.

Key Rollover

To support the changing of an MD5 key in an operational network without disrupting OSPF adjacencies (and hence the topology), a key rollover mechanism is supported. As a network administrator configures the new key into the multiple networking devices that communicate, some time exists when different devices are using both a new key and an old key. If an interface is configured with a new key, the software sends two copies of the same packet, each authenticated by the old key and new key. The software tracks which devices start using the new key, and the software stops sending duplicate packets after it detects that all of its neighbors are using the new key. The software then discards the old key. The network administrator must then remove the old key from each the configuration file of each router.

Neighbors and Adjacency for OSPF

Routers that share a segment (Layer 2 link between two interfaces) become neighbors on that segment. OSPF uses the hello protocol as a neighbor discovery and keep alive mechanism. The hello protocol involves receiving and periodically sending hello packets out each interface. The hello packets list all known OSPF neighbors on the interface. Routers become neighbors when they see themselves listed in the hello packet of the neighbor. After two routers are neighbors, they may proceed to exchange and synchronize their databases, which creates an adjacency. On broadcast and NBMA networks all neighboring routers have an adjacency.

Enabling strict-mode

The following procedure describes how to enable BFD strict-mode for Open Shortest Path First (OSPF) on an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0:hostname# configure`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**router ospf** *process-name* **Example:** `RP/0/RP0:hostname(config)# router ospf 1`	Enters OSPF configuration mode, allowing you to configure the OSPF routing process. Use the **show ospf** command in XR EXEC mode to obtain the process-name for the current router.
Step 3	**area** *area-id* **Example:** `RP/0/RP0:hostname(config-ospf)# area 0`	Configures an Open Shortest Path First (OSPF) area. Replace *area-id* with the OSPF area identifier.
Step 4	**interface** *type interface-path-id* **Example:** `RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE 0/6/0/6.11`	Enters interface configuration mode and specifies the interface name and notation *rack/slot/module/port*. The example indicates a Ten Gigabit Ethernet interface in modular services card slot 3.
Step 5	**bfd fast-detect strict-mode** **Example:** `RP/0/RP0:hostname(config-ospf-ar-if)# bfd fast-detect strict-mode`	Enables strict-mode to hold down neighbor session until BFD session is up.
Step 6	**commit**	Commits the changes to the running configuration.
Step 7	**show ospf interface** *type interface-path-id* **Example:** `RP/0/RP0:hostname(config-ospf-ar-if)#show ospf interface 0/6/0/6.11`	Verify that strict-mode is enabled on the appropriate interface.

BFD strict-mode: Example

The following example shows how to enable BFD strict-mode for OSPF on a Hundred Gigabit Ethernet interface and check the OSPF interface information. The value of **Mode** displays as **Strict** when BFD strict-mode is enabled. By default, the value of **Mode** displays as **Default**.

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#router ospf 0
RP/0/RP0:hostname(config-ospf)#area 0
RP/0/RP0:hostname(config-ospf-ar)#interface HundredGigE0/6/0/0.30
RP/0/RP0:hostname(config-ospf-ar-if)#bfd fast-detect strict-mode
RP/0/RP0:hostname(config-ospf-ar-if)#commit
RP/0/RP0:hostname(config-ospf-ar-if)#end
RP/0/RP0:hostname#show ospf interface HundredGigE0/6/0/0.30
```

```
HundredGigE0/6/0/0.30 is up, line protocol is up
  Internet Address 10.1.1.2/24, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, MTU 1500, MaxPktSz 1500
  BFD enabled, BFD interval 150 msec, BFD multiplier 3, Mode: Strict
  Designated Router (ID) 2.2.2.2, Interface address 10.1.1.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07:358
  Index 1/1, 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 1
  Neighbor Count is 1, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 0
```

The following example shows the output of the **show ospf neighbor** command. # indicates that the neighbor is waiting for the BFD session to come up.

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

Neighbors for OSPF 1

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1         0    DOWN/DROTHER    00:00:33    10.1.1.3/24        HundredGigE0/6/0/0.30#


Total neighbor count: 1
```

OSPF FIB Download Notification

OSPF FIB Download Notification feature minimizes the ingress traffic drop for a prolonged period of time after the line card reloads and this feature is enabled by default.

Open Shortest Path First (OSPF) registers with Routing Information Base (RIB) through Interface Table Attribute Library (ITAL) which keeps the interface down until all the routes are downloaded to Forwarding Information Base (FIB). OSPF gets the Interface Up notification when all the routes on the reloaded line card are downloaded through RIB/FIB.

RIB provides notification to registered clients when a:

- Node is lost.
- Node is created.
- Node's FIB upload is completed.

Designated Router (DR) for OSPF

On point-to-point and point-to-multipoint networks, the Cisco IOS XR software floods routing updates to immediate neighbors. No DR or backup DR (BDR) exists; all routing information is flooded to each router.

On broadcast or NBMA segments only, OSPF minimizes the amount of information being exchanged on a segment by choosing one router to be a DR and one router to be a BDR. Thus, the routers on the segment have a central point of contact for information exchange. Instead of each router exchanging routing updates with every other router on the segment, each router exchanges information with the DR and BDR. The DR and BDR relay the information to the other routers.

The software looks at the priority of the routers on the segment to determine which routers are the DR and BDR. The router with the highest priority is elected the DR. If there is a tie, then the router with the higher router ID takes precedence. After the DR is elected, the BDR is elected the same way. A router with a router priority set to zero is ineligible to become the DR or BDR.

Default Route for OSPF

Type 5 (ASE) LSAs are generated and flooded to all areas except stub areas. For the routers in a stub area to be able to route packets to destinations outside the stub area, a default route is injected by the ABR attached to the stub area.

The cost of the default route is 1 (default) or is determined by the value specified in the **default-cost** command.

Link-State Advertisement Types for OSPF Version 2

Each of the following LSA types has a different purpose:

- Router LSA (Type 1)—Describes the links that the router has within a single area, and the cost of each link. These LSAs are flooded within an area only. The LSA indicates if the router can compute paths based on quality of service (QoS), whether it is an ABR or ASBR, and if it is one end of a virtual link. Type 1 LSAs are also used to advertise stub networks.
- Network LSA (Type 2)—Describes the link state and cost information for all routers attached to a multiaccess network segment. This LSA lists all the routers that have interfaces attached to the network segment. It is the job of the designated router of a network segment to generate and track the contents of this LSA.
- Summary LSA for ABRs (Type 3)—Advertises internal networks to routers in other areas (interarea routes). Type 3 LSAs may represent a single network or a set of networks aggregated into one prefix. Only ABRs generate summary LSAs.
- Summary LSA for ASBRs (Type 4)—Advertises an ASBR and the cost to reach it. Routers that are trying to reach an external network use these advertisements to determine the best path to the next hop. ABRs generate Type 4 LSAs.
- Autonomous system external LSA (Type 5)—Redistributes routes from another autonomous system, usually from a different routing protocol into OSPF.
- Autonomous system external LSA (Type 7)—Provides for carrying external route information within an NSSA. Type 7 LSAs may be originated by and advertised throughout an NSSA. NSSAs do not receive or originate Type 5 LSAs. Type 7 LSAs are advertised only within a single NSSA. They are not flooded into the backbone area or into any other area by border routers.
- Intra-area-prefix LSAs (Type 9)—A router can originate multiple intra-area-prefix LSAs for every router or transit network, each with a unique link-state ID. The link-state ID for each intra-area-prefix LSA describes its association to either the router LSA or network LSA and contains prefixes for stub and transit networks.
- Area local scope (Type 10)—Opaque LSAs are not flooded past the borders of their associated area.
- Link-state (Type 11)—The LSA is flooded throughout the AS. The flooding scope of Type 11 LSAs are equivalent to the flooding scope of AS-external (Type 5) LSAs. Similar to Type 5 LSAs, the LSA is rejected if a Type 11 opaque LSA is received in a stub area from a neighboring router within the stub area. Type 11 opaque LSAs have these attributes:

- LSAs are flooded throughout all transit areas.
- LSAs are not flooded into stub areas from the backbone.
- LSAs are not originated by routers into their connected stub areas.

Virtual Link and Transit Area for OSPF

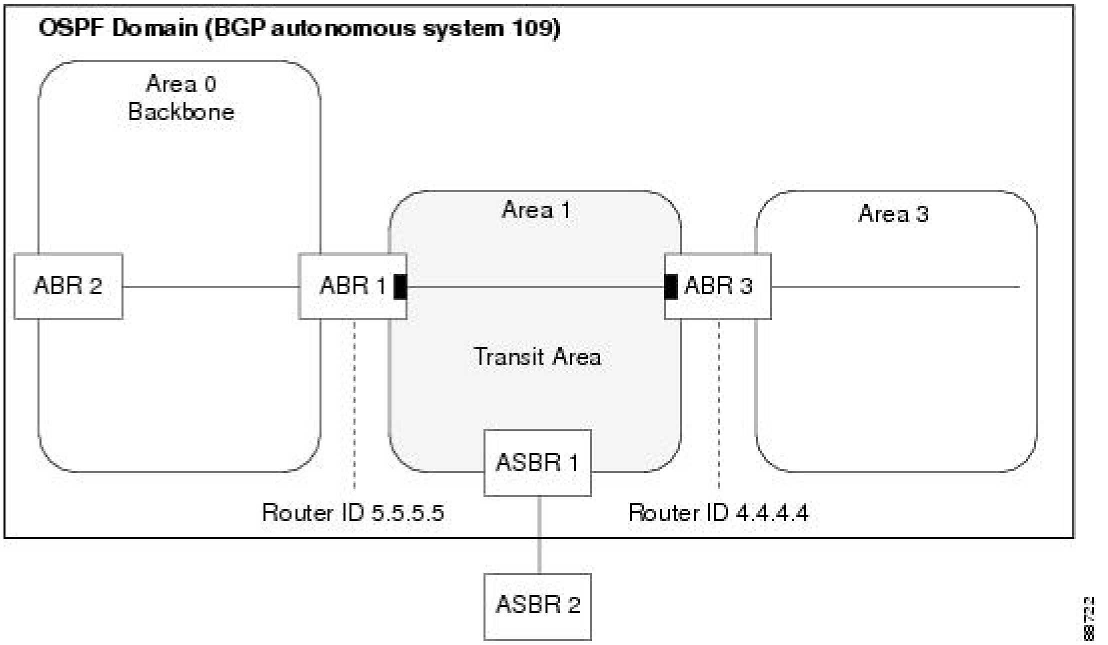
In OSPF, routing information from all areas is first summarized to the backbone area by ABRs. The same ABRs, in turn, propagate such received information to their attached areas. Such hierarchical distribution of routing information requires that all areas be connected to the backbone area (Area 0). Occasions might exist for which an area must be defined, but it cannot be physically connected to Area 0. Examples of such an occasion might be if your company makes a new acquisition that includes an OSPF area, or if Area 0 itself is partitioned.

In the case in which an area cannot be connected to Area 0, you must configure a virtual link between that area and Area 0. The two endpoints of a virtual link are ABRs, and the virtual link must be configured in both routers. The common nonbackbone area to which the two routers belong is called a transit area. A virtual link specifies the transit area and the router ID of the other virtual endpoint (the other ABR).

A virtual link cannot be configured through a stub area or NSSA.

Figure 13: Virtual Link to Area 0

This figure illustrates a virtual link from Area 3 to Area 0.



Passive Interface

Setting an interface as passive disables the sending of routing updates for the neighbors, hence adjacencies will not be formed in OSPF. However, the particular subnet will continue to be advertised to OSPF neighbors.

Use the **passive** command in appropriate mode to suppress the sending of OSPF protocol operation on an interface.

It is recommended to use passive configuration on interfaces that are connecting LAN segments with hosts to the rest of the network, but are not meant to be transit links between routers.

OSPFv2 SPF Prefix Prioritization

The OSPFv2 SPF Prefix Prioritization feature enables an administrator to converge, in a faster mode, important prefixes during route installation.

When a large number of prefixes must be installed in the Routing Information Base (RIB) and the Forwarding Information Base (FIB), the update duration between the first and last prefix, during SPF, can be significant.

In networks where time-sensitive traffic (for example, VoIP) may transit to the same router along with other traffic flows, it is important to prioritize RIB and FIB updates during SPF for these time-sensitive prefixes.

The OSPFv2 SPF Prefix Prioritization feature provides the administrator with the ability to prioritize important prefixes to be installed, into the RIB during SPF calculations. Important prefixes converge faster among prefixes of the same route type per area. Before RIB and FIB installation, routes and prefixes are assigned to various priority batch queues in the OSPF local RIB, based on specified route policy. The RIB priority batch queues are classified as "critical," "high," "medium," and "low," in the order of decreasing priority.

When enabled, prefix alters the sequence of updating the RIB with this prefix priority:

Critical > High > Medium > Low

As soon as prefix priority is configured, /32 prefixes are no longer preferred by default; they are placed in the low-priority queue, if they are not matched with higher-priority policies. Route policies must be devised to retain /32s in the higher-priority queues (high-priority or medium-priority queues).

Priority is specified using route policy, which can be matched based on IP addresses or route tags. During SPF, a prefix is checked against the specified route policy and is assigned to the appropriate RIB batch priority queue.

These are examples of this scenario:

- If only high-priority route policy is specified, and no route policy is configured for a medium priority:
  - Permitted prefixes are assigned to a high-priority queue.
  - Unmatched prefixes, including /32s, are placed in a low-priority queue.
- If both high-priority and medium-priority route policies are specified, and no maps are specified for critical priority:
  - Permitted prefixes matching high-priority route policy are assigned to a high-priority queue.
  - Permitted prefixes matching medium-priority route policy are placed in a medium-priority queue.
  - Unmatched prefixes, including /32s, are moved to a low-priority queue.
- If both critical-priority and high-priority route policies are specified, and no maps are specified for medium priority:
  - Permitted prefixes matching critical-priority route policy are assigned to a critical-priority queue.
  - Permitted prefixes matching high-priority route policy are assigned to a high-priority queue.

  - Unmatched prefixes, including /32s, are placed in a low-priority queue.

- If only medium-priority route policy is specified and no maps are specified for high priority or critical priority:
  - Permitted prefixes matching medium-priority route policy are assigned to a medium-priority queue.
  - Unmatched prefixes, including /32s, are placed in a low-priority queue.

Use the **[no] spf prefix-priority route-policy** *rpl* command to prioritize OSPFv2 prefix installation into the global RIB during SPF.

SPF prefix prioritization is disabled by default. In disabled mode, /32 prefixes are installed into the global RIB, before other prefixes. If SPF 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 /32s, are placed in the low-priority queue.

If all /32s are desired in the high-priority queue or medium-priority queue, configure this single route map:

```
prefix-set ospf-medium-prefixes
  0.0.0.0/0 ge 32
  end-set
```

Route Redistribution for OSPF

Redistribution allows different routing protocols to exchange routing information. This technique can be used to allow connectivity to span multiple routing protocols. It is important to remember that the **redistribute** command controls redistribution *into* an OSPF process and not from OSPF. See Configuration Examples for Implementing OSPF , on page 471 for an example of route redistribution for OSPF.

OSPF Shortest Path First Throttling

OSPF SPF throttling makes it possible to configure SPF scheduling in millisecond intervals and to potentially delay SPF calculations during network instability. SPF is scheduled to calculate the Shortest Path Tree (SPT) when there is a change in topology. One SPF run may include multiple topology change events.

The interval at which the SPF calculations occur is chosen dynamically and based on the frequency of topology changes in the network. The chosen interval is within the boundary of the user-specified value ranges. If network topology is unstable, SPF throttling calculates SPF scheduling intervals to be longer until topology becomes stable.

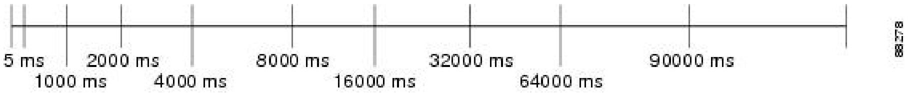
SPF calculations occur at the interval set by the **timers throttle spf** command. The wait interval indicates the amount of time to wait until the next SPF calculation occurs. Each wait interval after that calculation is twice as long as the previous interval until the interval reaches the maximum wait time specified.

The SPF timing can be better explained using an example. In this example, the start interval is set at 5 milliseconds (ms), initial wait interval at 1000 ms, and maximum wait time at 90,000 ms.

```
  timers spf 5 1000 90000
```

Figure 14: SPF Calculation Intervals Set by the timers spf Command

This figure shows the intervals at which the SPF calculations occur as long as at least one topology change event is received in a given wait interval.

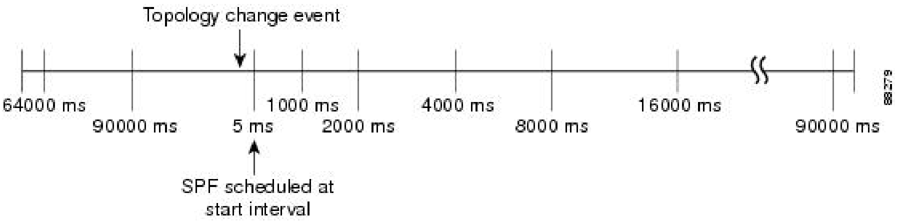


Notice that the wait interval between SPF calculations doubles when at least one topology change event is received during the previous wait interval. After the maximum wait time is reached, the wait interval remains the same until the topology stabilizes and no event is received in that interval.

If the first topology change event is received after the current wait interval, the SPF calculation is delayed by the amount of time specified as the start interval. The subsequent wait intervals continue to follow the dynamic pattern.

If the first topology change event occurs after the maximum wait interval begins, the SPF calculation is again scheduled at the start interval and subsequent wait intervals are reset according to the parameters specified in the **timers throttle spf** command. Notice in Figure 15: Timer Intervals Reset After Topology Change Event, on page 423that a topology change event was received after the start of the maximum wait time interval and that the SPF intervals have been reset.

Figure 15: Timer Intervals Reset After Topology Change Event



Information About Implementing OSPF

To implement OSPF you need to understand the following concepts:

Warm Standby and Nonstop Routing for OSPF Version 2

OSPFv2 warm standby provides high availability across RP switchovers. With warm standby extensions, each process running on the active RP has a corresponding standby process started on the standby RP. A standby OSPF process can send and receive OSPF packets with no performance impact to the active OSPF process.

Nonstop routing (NSR) allows an RP failover, process restart, or in-service upgrade to be invisible to peer routers and ensures that there is minimal performance or processing impact. Routing protocol interactions between routers are not impacted by NSR. NSR is built on the warm standby extensions. NSR alleviates the requirement for Cisco NSF and IETF graceful restart protocol extensions.

Note It is recommended to set the hello timer interval to the default of 10 seconds. OSPF sessions may flap during switchover if hello-interval timer configured is less then default value.

Multicast-Intact Support for OSPF

The multicast-intact feature provides the ability to run multicast routing (PIM) when IGP shortcuts are configured and active on the router. Both OSPFv2 and IS-IS support the multicast-intact feature.

You can enable multicast-intact in the IGP when multicast routing protocols (PIM) are configured and IGP shortcuts are configured on the router. IGP shortcuts are MPLS tunnels that are exposed to IGP. The IGP routes IP traffic over these tunnels to destinations that are downstream from the egress router of the tunnel (from an SPF perspective). PIM cannot use IGP shortcuts for propagating PIM joins, because reverse path forwarding (RPF) cannot work across a unidirectional tunnel.

When you enable multicast-intact on an IGP, the IGP publishes a parallel or alternate set of equal-cost next hops for use by PIM. These next hops are called *mcast-intact* next hops. The mcast-intact next hops have the following attributes:

- They are guaranteed not to contain any IGP shortcuts.
- They are not used for unicast routing but are used only by PIM to look up an IPv4 next-hop to a PIM source.
- They are not published to the FIB.
- When multicast-intact is enabled on an IGP, all IPv4 destinations that were learned through link-state advertisements are published with a set equal-cost mcast-intact next hops to the RIB. This attribute applies even when the native next hops have no IGP shortcuts.

In OSPF, the max-paths (number of equal-cost next hops) limit is applied separately to the native and mcast-intact next hops. The number of equal cost mcast-intact next hops is the same as that configured for the native next hops.

Configure Prefix Suppression for OSPF

Transit-only networks that connect two routers are usually configured with routing IP addresses that are advertised in the Links State Advertisements (LSAs). However, these prefixes are not needed for data traffic. Suppressing these prefixes would reduce the number of links in LSAs, thereby improving convergence and also reducing the vulnerability of potential remote attacks.

Prefixes can be suppressed for an OSPF process, an OSPF area, or for specific interfaces of a router.

Configure Prefix Suppression for a Router Running OSPF

Use the procedure in this section to configure prefix suppression for an OSPF process on a router.

Note

- If you suppress prefixes for an OSPF process on a router, the suppression is valid for all interfaces and areas associated with the router.
- When prefix suppression is configured on an NSSA ASBR, all interfaces on the routers have their prefixes suppressed, and the Type 7 LSAs have a forwarding address of 0. This would stop the translation of Type 7 LSAs to Type 5 by the NSSA ABR. The workaround for this is to configure at least one loopback interface in the NSSA area, or one interface with prefix suppression disabled, so that the interface address is selected as the forwarding address for all the Type 7 LSAs.

1. Enter the global configuration mode and configure the interfaces of the 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 10.1.1.1 255.255.255.0
RP/0/RP0:hostname(config-if)# no shut
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Loopback 0
RP/0/RP0:hostname(config-if)# ipv4 address 10.10.10.10 255.255.255.255
RP/0/RP0:hostname(config-if)# no shut
RP/0/RP0:hostname(config-if)# exit
```

2. Configure the OSPF process with prefix suppression.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf pfx
RP/0/RP0:hostname(config-ospf)# router-id 10.10.10.10
RP/0/RP0:hostname(config-ospf)# prefix-suppression
```

3. Add the configured interfaces to the OSPF area.

```
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# interface Loopback 0
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# network point-to-point
```

4. Exit the OSPF area configuration mode and commit your configuration.

```
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# exit
RP/0/RP0:hostname(config-ospf)# exit
RP/0/RP0:hostname(config)# commit
RP/0/RP0:hostname(config)# exit
```

5. Confirm your configuration.

```
RP/0/RP0:hostname# show running-configuration
...
interface Loopback0
 ipv4 address 10.10.10.10 255.255.255.255
!
interface TenGigE0/6/0/2.10
 ipv4 address 10.1.1.1 255.255.255.0
!
router ospf pfx
 router-id 10.10.10.10
 prefix-suppression
 area 0
  interface TenGigE0/6/0/2.10
   network point-to-point
  !
 !
!
```

6. Verify if prefix suppression is enabled.

```
RP/0/RP0:hostname# show ospf interface
Fri Jun 17 15:13:08.470 IST

Interfaces for OSPF 1

TenGigE0/6/0/2.10 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0
  Process ID 1, Router ID 10.10.10.10, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1, MTU 1500, MaxPktSz 1500
  Designated Router (ID) 10.10.10.20, Interface address 10.1.1.2
  Backup Designated router (ID) 10.10.10.30, Interface address 10.1.1.3
  Primary addresses not advertised
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06:898
  Index 2/2, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  LS Ack List: current length 0, high water mark 2
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.10.10.30  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 0
```

If your output verifies that primary addresses are not advertised, then you have successfully configured prefix suppression for the OSPF process on the router.

Configure Prefix Suppression for an OSPF Area

Use the procedure in this section to configure prefix suppression for an OSPF area.

Note If you suppress prefixes on an area, the suppression is valid for all interfaces associated with the area.

1. Enter the global configuration mode and configure the interfaces of the 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 10.1.1.1 255.255.255.0
RP/0/RP0:hostname(config-if)# no shut
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Loopback 0
RP/0/RP0:hostname(config-if)# ipv4 address 10.10.10.10 255.255.255.255
RP/0/RP0:hostname(config-if)# no shut
RP/0/RP0:hostname(config-if)# exit
```

2. Configure the OSPF area with prefix suppression.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf pfx
RP/0/RP0:hostname(config-ospf)# router-id 10.10.10.10
RP/0/RP0:hostname(config-ospf)# area 0
RP/0/RP0:hostname(config-ospf-ar)# prefix-suppression
```

3. Add the configured interfaces to the OSPF area.

```
RP/0/RP0:hostname(config-ospf-ar)# interface Loopback 0
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# network point-to-point
```

4. Exit the OSPF area configuration mode and commit your configuration.

```
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# exit
RP/0/RP0:hostname(config-ospf)# exit
RP/0/RP0:hostname(config)# commit
RP/0/RP0:hostname(config)# exit
```

5. Confirm your configuration.

```
RP/0/RP0:hostname# show running-configuration
...
interface Loopback0
 ipv4 address 10.10.10.10 255.255.255.255
!
interface TenGigE0/6/0/2.10
 ipv4 address 10.1.1.1 255.255.255.0
!
router ospf pfx
 router-id 10.10.10.10
 area 0
  prefix-suppression
  interface TenGigE0/6/0/2.10
   network point-to-point
  !
 !
!
```

6. Verify if prefix suppression is enabled.

```
RP/0/RP0:hostname# show ospf interface
Fri Jun 17 15:13:08.470 IST

Interfaces for OSPF 1

TenGigE0/6/0/2.10 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0
  Process ID 1, Router ID 10.10.10.10, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1, MTU 1500, MaxPktSz 1500
  Designated Router (ID) 10.10.10.20, Interface address 10.1.1.2
  Backup Designated router (ID) 10.10.10.30, Interface address 10.1.1.3
  Primary addresses not advertised
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06:898
  Index 2/2, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  LS Ack List: current length 0, high water mark 2
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.10.10.30  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 0
```

If your output verifies that primary addresses are not advertised, then you have successfully configured prefix suppression for the OSPF area.

Configure Prefix Suppression for an OSPF Interface

Use the procedure in this section to configure prefix suppression for an OSPF interface.

Note If you suppress prefixes on an interface, suppression is valid only on that interface, and all other interfaces must be configured separately with prefix suppression.

1. Enter the global configuration mode and configure the interfaces of the 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 10.1.1.1 255.255.255.0
RP/0/RP0:hostname(config-if)# no shut
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Loopback 0
RP/0/RP0:hostname(config-if)# ipv4 address 10.10.10.10 255.255.255.255
RP/0/RP0:hostname(config-if)# no shut
RP/0/RP0:hostname(config-if)# exit
```

2. Configure the OSPF area.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# router ospf pfx
RP/0/RP0:hostname(config-ospf)# router-id 10.10.10.10
RP/0/RP0:hostname(config-ospf)# area 0
```

3. Add the configured interfaces to the OSPF area, and configure prefix suppression on the required interface.

```
RP/0/RP0:hostname(config-ospf-ar)# interface Loopback 0
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
RP/0/RP0:hostname(config-ospf-ar-if)# network point-to-point
RP/0/RP0:hostname(config-ospf-ar-if)# prefix-suppression
```

4. Exit the OSPF area configuration mode and commit your configuration.

```
RP/0/RP0:hostname(config-ospf-ar-if)# exit
RP/0/RP0:hostname(config-ospf-ar)# exit
RP/0/RP0:hostname(config-ospf)# exit
RP/0/RP0:hostname(config)# commit
RP/0/RP0:hostname(config)# exit
```

5. Confirm your configuration.

```
RP/0/RP0:hostname# show running-configuration
...
interface Loopback0
 ipv4 address 10.10.10.10 255.255.255.255
!
interface TenGigE0/6/0/2.10
 ipv4 address 10.1.1.1 255.255.255.0
!
router ospf pfx
 router-id 10.10.10.10
 area 0
  interface TenGigE0/6/0/2.10
   network point-to-point
   prefix-suppression
  !
 !
!
```

6. Verify if prefix suppression is enabled.

```
RP/0/RP0:hostname# show ospf interface
Fri Jun 17 15:13:08.470 IST

Interfaces for OSPF 1

TenGigE0/6/0/2.10 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0
  Process ID 1, Router ID 10.10.10.10, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1, MTU 1500, MaxPktSz 1500
  Designated Router (ID) 10.10.10.20, Interface address 10.1.1.2
  Backup Designated router (ID) 10.10.10.30, Interface address 10.1.1.3
  Primary addresses not advertised
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06:898
Index 2/2, flood queue length 0
Next 0(0)/0(0)
Last flood scan length is 2, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
LS Ack List: current length 0, high water mark 2
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.10.10.30  (Designated Router)
Suppress hello for 0 neighbor(s)
Multi-area interface Count is 0
```

If your output verifies that primary addresses are not advertised, then you have successfully configured prefix suppression on the interface.

Multi-Area Adjacency for OSPF Version 2

The multi-area adjacency feature for OSPFv2 allows a link to be configured on the primary interface in more than one area so that the link could be considered as an intra-area link in those areas and configured as a preference over more expensive paths.

This feature establishes a point-to-point unnumbered link in an OSPF area. A point-to-point link provides a topological path for that area, and the primary adjacency uses the link to advertise the link consistent with draft-ietf-ospf-multi-area-adj-06.

The following are multi-area interface attributes and limitations:

- Exists as a logical construct over an existing primary interface for OSPF; however, the neighbor state on the primary interface is independent of the multi-area interface.
- Establishes a neighbor relationship with the corresponding multi-area interface on the neighboring router. A mixture of multi-area and primary interfaces is not supported.
- Advertises an unnumbered point-to-point link in the router link state advertisement (LSA) for the corresponding area when the neighbor state is full.
- Created as a point-to-point network type. 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.
- Inherits the Bidirectional Forwarding Detection (BFD) characteristics from its primary interface. BFD is not configurable under a multi-area interface; however, it is configurable under the primary interface.

The multi-area interface inherits the interface characteristics from its primary interface, but some interface characteristics can be configured under the multi-area interface configuration mode as shown below:

```
RP/0/RP0:hostname(config-ospf-ar)# multi-area-interface TenGigE0/3/0/9.21
RP/0/RP0:hostname(config-ospf-ar-mif)# ?
  authentication       Enable authentication
  authentication-key   Authentication password (key)
  cost                 Interface cost
  cost-fallback        Cost when cumulative bandwidth goes below the theshold
  database-filter      Filter OSPF LSA during synchronization and flooding
  dead-interval        Interval after which a neighbor is declared dead
  distribute-list      Filter networks in routing updates
  hello-interval       Time between HELLO packets
  message-digest-key   Message digest authentication password (key)
  mtu-ignore           Enable/Disable ignoring of MTU in DBD packets
  packet-size          Customize size of OSPF packets upto MTU
  retransmit-interval  Time between retransmitting lost link state advertisements
  transmit-delay       Estimated time needed to send link-state update packet

RP/0/RP0:hostname(config-ospf-ar-mif)#
```

OSPF Authentication Message Digest Management

All OSPF routing protocol exchanges are authenticated and the method used can vary depending on how authentication is configured. When using cryptographic authentication, the OSPF routing protocol uses the Message Digest 5 (MD5) authentication algorithm to authenticate packets transmitted between neighbors in the network. For each OSPF protocol packet, a key is used to generate and verify a message digest that is appended to the end of the OSPF packet. The message digest is a one-way function of the OSPF protocol packet and the secret key. Each key is identified by the combination of interface used and the key identification. An interface may have multiple keys active at any time.

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.

GTSM TTL Security Mechanism for OSPF

OSPF is a link state protocol that requires networking devices to detect topological changes in the network, flood Link State Advertisement (LSA) updates to neighbors, and quickly converge on a new view of the topology. However, during the act of receiving LSAs from neighbors, network attacks can occur, because there are no checks that unicast packets are originating from a neighbor that is one hop away or multiple hops away over virtual links.

For virtual links, OSPF packets travel multiple hops across the network; hence, the TTL value can be decremented several times. For these type of links, a minimum TTL value must be allowed and accepted for multiple-hop packets.

To filter network attacks originating from invalid sources traveling over multiple hops, the Generalized TTL Security Mechanism (GTSM), RFC 3682, is used to prevent the attacks. GTSM filters link-local addresses and allows for only one-hop neighbor adjacencies through the configuration of TTL value 255. The TTL value in the IP header is set to 255 when OSPF packets are originated, and checked on the received OSPF packets against the default GTSM TTL value 255 or the user configured GTSM TTL value, blocking unauthorized OSPF packets originated from TTL hops away.

Path Computation Element for OSPFv2

A PCE is an entity (component, application, or network node) that is capable of computing a network path or route based on a network graph and applying computational constraints.

PCE is accomplished when a PCE address and client is configured for MPLS-TE. PCE communicates its PCE address and capabilities to OSPF then OSPF packages this information in the PCE Discovery type-length-value (TLV) (Type 2) and reoriginates the RI LSA. OSPF also includes the Router Capabilities TLV (Type 1) in all its RI LSAs. The PCE Discovery TLV contains the PCE address sub-TLV (Type 1) and the Path Scope Sub-TLV (Type 2).

The PCE Address Sub-TLV specifies the IP address that must be used to reach the PCE. It should be a loop-back address that is always reachable, this TLV is mandatory, and must be present within the PCE Discovery TLV. The Path Scope Sub-TLV indicates the PCE path computation scopes, which refers to the PCE ability to compute or participate in the computation of intra-area, inter-area, inter-AS or inter-layer TE LSPs.

PCE extensions to OSPFv2 include support for the Router Information Link State Advertisement (RI LSA). OSPFv2 is extended to receive all area scopes (LSA Types 9, 10, and 11). However, OSPFv2 originates only area scope Type 10.

OSPF IP Fast Reroute Loop Free Alternate

The OSPF IP Fast Reroute (FRR) Loop Free Alternate (LFA) computation supports these:

- Fast rerouting capability by using IP forwarding and routing
- Handles failure in the line cards in minimum time

OSPF Over GRE Interfaces

Cisco IOS XR software provides the capability to run OSPF protocols over Generic Routing Encapsulation (GRE) tunnel interfaces.

VRF-lite Support for OSPFv2

VRF-lite capability is enabled for OSPF version 2 (OSPFv2). VRF-lite is the virtual routing and forwarding (VRF) deployment without the BGP/MPLS based backbone. In VRF-lite, individual provider edge (PE) routers are directly connected using VRF interfaces. To enable VRF-lite in OSPFv2, configure the **capability vrf-lite** command in VRF configuration mode. When VRF-lite is configured, the DN bit processing and the automatic Area Border Router (ABR) status setting are disabled.

OSPFv2 Unequal Cost Load Balancing

Unequal Cost Load Balancing feature in Cisco IOS XR OSPFv2 feature enables Unequal Cost Multipath (UCMP) calculation based on configured prefix-list and based on variance factor. UCMP path can be calculated for all prefixes or only for selected prefixes based on the configuration. Selected interfaces can be excluded to be used as a candidate for UCMP paths. The calculated UCMP paths are then installed in the routing information base (RIB) subject to the max-path limit.

The OSPFv2 interior gateway protocol is used to calculate paths to prefixes inside an autonomous system. OSPF calculates up to maximum paths (max-path) equal cost multi-paths (ECMPs) for each prefix, where max-path is either limited by the router support or is configured by the user.

UCMP Paths Calculation

In some topologies, alternate paths to prefix exist even though their metric is higher then the metric of the best path(s). These paths are called Unequal Cost Multipaths (UCMPs). These paths are guaranteed to be loop free. Users can send some portion of the traffic down these paths to better utilize the available bandwidth. However, the UCMP paths are not discovered by the traditional Dijkstra calculation. Additional computation is required to discover these paths.

Unequal Cost Multipath Load-balancing for OSPF

The unequal cost multipath (UCMP) load-balancing adds the capability with Open Shortest Path First (OSPF) to load-balance traffic proportionally across multiple paths, with different cost. Without UCMP enabled, only the best cost paths are discovered by OSPF (ECMP) and alternate higher cost paths are not computed.

Generally, higher bandwidth links have lower IGP metrics configured, so that they form the shortest IGP paths. With the UCMP load-balancing enabled, IGP can use even lower bandwidth links or higher cost links for traffic, and can install these paths to the forwarding information base (FIB). OSPF installs multiple paths to the same destination in FIB, but each path will have a 'load metric/weight' associated with it. FIB uses this load metric/weight to decide the amount of traffic that needs to be sent on a higher bandwidth path and the amount of traffic that needs to be sent on a lower bandwidth path.

The UCMP computation is provided under OSPF VRF context, enabling UCMP computation for a particular VRF. For default VRF the configuration is done under the OSPF global mode. The UCMP configuration is also provided with a prefix-list option, which would limit the UCMP computation only for the prefixes present in the prefix-list. If prefix-list option is not provided, UCMP computation is done for the reachable prefixes in OSPF. The number of UCMP paths to be considered and installed is controlled using the **variance** configuration. Variance value identifies the range for the UCMP path metric to be considered for installation into routing information base (RIB/FIB) and is defined in terms of a percentage of the primary path metric. Total number of paths, including ECMP and UCMP paths together is limited by the max-path configuration or by the max-path capability of the platform.

There is an option to exclude an interface from being used for UCMP computation. If it is desired that a particular interface should not be considered as a UCMP nexthop, for any prefix, then use the UCMP **exclude interface** command to configure the interface to be excluded from UCMP computation.

Enabling the UCMP configuration indicates that OSPF should perform UCMP computation for the all the reachable OSPF prefixes or all the prefixes permitted by the prefix-list, if the prefix-list option is used. The UCMP computation happens only after the primary SPF and route calculation is completed. There would be a configurable delay (default delay is 100 ms) from the time primary route calculation is completed and UCMP computation is started. Use the UCMP **delay-interval** command to configure the delay between primary SPF completion and start of UCMP computation. UCMP computation will be done during the fast re-route computation (IPFRR does not need to be enabled for UCMP computation to be performed). If IPFRR is enabled, the fast re-route backup paths will be calculated for both the primary equal cost multipath (ECMP) paths and the UCMP paths.

To manually adjust UCMP ratio, use any command that changes the metric of the link.

- By using the bandwidth command in interface configuration mode
- By adjusting the OSPF interface cost on the link

How to Implement OSPF

This section contains the following procedures:

Enabling OSPF

This task explains how to perform the minimum OSPF configuration on your router that is to enable an OSPF process with a router ID, configure a backbone or nonbackbone area, and then assign one or more interfaces on which OSPF runs.

Before you begin

Although you can configure OSPF before you configure an IP address, no OSPF routing occurs until at least one IP address is configured.

Procedure

Step 1 **configure**

Step 2 **router ospf**

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IP address as the router ID.

Step 4 **area** *area-id*

Example:

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

Enters area configuration mode and configures an area for the OSPF process.

- Backbone areas have an area ID of 0.
- Nonbackbone areas have a nonzero area ID.
- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 5 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces for the area configured in Step 4.

Step 6 Repeat Step 5 for each interface that uses OSPF.

—

Step 7 **log adjacency changes** [**detail**] [**enable** | **disable**]

Example:

```
RP/0/RP0:hostname(config-ospf-ar-if)# log adjacency changes detail
```

(Optional) Requests notification of neighbor changes.

- By default, this feature is enabled.
- The messages generated by neighbor changes are considered notifications, which are categorized as severity Level 5 in the **logging console** command. The **logging console** command controls which severity level of messages are sent to the console. By default, all severity level messages are sent.

Step 8 **commit**

Configuring Stub and Not-So-Stubby Area Types

This task explains how to configure the stub area and the NSSA for OSPF.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IP address as the router ID.

Step 4 **area** *area-id*

Example:

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

Enters area configuration mode and configures a nonbackbone area for the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 5 Do one of the following:

- **stub** [**no-summary**]
- **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# stub no summary
```

or

```
RP/0/RP0:hostname(config-ospf-ar)# nssa no-redistribution
```

Defines the nonbackbone area as a stub area.

- Specify the **no-summary** keyword to further reduce the number of LSAs sent into a stub area. This keyword prevents the ABR from sending summary link-state advertisements (Type 3) in the stub area.

or

Defines an area as an NSSA.

Step 6 Do one of the following:

- **stub**
- **nssa**

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# stub
```

or

```
RP/0/RP0:hostname(config-ospf-ar)# nssa
```

(Optional) Turns off the options configured for stub and NSSA areas.

- If you configured the stub and NSSA areas using the optional keywords (**no-summary** , **no-redistribution** , **default-information-originate** , and **no-summary**) in Step 5, you must now reissue the **stub** and **nssa** commands without the keywords—rather than using the **no** form of the command.
- For example, the **no nssa default-information-originate** form of the command changes the NSSA area into a normal area that inadvertently brings down the existing adjacencies in that area.

Step 7 **default-cost** *cost*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)#default-cost 15
```

(Optional) Specifies a cost for the default summary route sent into a stub area or an NSSA.

- Use this command only on ABRs attached to the NSSA. Do not use it on any other routers in the area.
- The default cost is 1.

Step 8 **commit**

Step 9 Repeat this task on all other routers in the stub area or NSSA.

—

Configuring Neighbors for Nonbroadcast Networks

This task explains how to configure neighbors for a nonbroadcast network. This task is optional.

Before you begin

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed network.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IP address as the router ID.

Step 4 **area** *area-id*

Example:

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

Enters area configuration mode and configures an area for the OSPF process.

- The example configures a backbone area.
- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 5 **network** { **broadcast** | **non-broadcast** | { **point-to-multipoint** [**non-broadcast**] | **point-to-point** }}

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# network non-broadcast
```

Configures the OSPF network type to a type other than the default for a given medium.

- The example sets the network type to NBMA.

Step 6 **dead-interval** *seconds*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# dead-interval 40
```

(Optional) Sets the time to wait for a hello packet from a neighbor before declaring the neighbor down.

Step 7 **hello-interval** *seconds*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# hello-interval 10
```

(Optional) Specifies the interval between hello packets that OSPF sends on the interface.

Note It is recommended to set the hello timer interval to the default of 10 seconds. OSPF sessions may flap during switchover if hello-interval timer configured is less then default value.

Step 8 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces for the area configured in Step 4.

- In this example, the interface inherits the nonbroadcast network type and the hello and dead intervals from the areas because the values are not set at the interface level.

Step 9 **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*][**cost** *number*]

Example:

```
RP/0/RP0:hostname(config-ospf-ar-if)# neighbor 10.20.20.1 priority 3 poll-interval 15
```

Configures the IPv4 address of OSPF neighbors interconnecting to nonbroadcast networks.

- The *ipv6-link-local-address* argument must be in the form documented in RFC 2373 in which the address is specified in hexadecimal using 16-bit values between colons.
- The **priority** keyword notifies the router that this neighbor is eligible to become a DR or BDR. The priority value should match the actual priority setting on the neighbor router. The neighbor priority default value is zero. This keyword does not apply to point-to-multipoint interfaces.
- The **poll-interval** keyword does not apply to point-to-multipoint interfaces. RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes).
- Neighbors with no specific cost configured assumes 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 NBMA networks.

- The **database-filter** keyword filters outgoing LSAs to an OSPF neighbor. If you specify the **all** keyword, incoming and outgoing LSAs are filtered. Use with extreme caution since filtering may cause the routing topology to be seen as entirely different between two neighbors, resulting in an unwanted traffic drop or routing loops.

Step 10 Repeat Step 9 for all neighbors on the interface.

—

Step 11 exit

Example:

```
RP/0/RP0:hostname(config-ospf-ar-if)# exit
```

Enters area configuration mode.

Step 12 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
```

Enters interface configuration mode and associates one or more interfaces for the area configured in Step 4.

- In this example, the interface inherits the nonbroadcast network type and the hello and dead intervals from the areas because the values are not set at the interface level.

Step 13 **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*][**cost** *number*] [**database-filter** [**all**]]

Example:

```
RP/0/
/CPU0:router(config-ospf-ar)# neighbor 10.34.16.6
```

Configures the IPv4 address of OSPF neighbors interconnecting to nonbroadcast networks.

- The *ipv6-link-local-address* argument must be in the form documented in RFC 2373 in which the address is specified in hexadecimal using 16-bit values between colons.
- The **priority** keyword notifies the router that this neighbor is eligible to become a DR or BDR. The priority value should match the actual priority setting on the neighbor router. The neighbor priority default value is zero. This keyword does not apply to point-to-multipoint interfaces.
- The **poll-interval** keyword does not apply to point-to-multipoint interfaces. RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes).
- Neighbors with no specific cost configured assumes 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 NBMA networks.
- The **database-filter** keyword filters outgoing LSAs to an OSPF neighbor. If you specify the **all** keyword, incoming and outgoing LSAs are filtered. Use with extreme caution since filtering may cause the routing topology to be seen as entirely different between two neighbors, resulting in an unwanted traffic drop or routing loops.

Step 14 Repeat Step 13 for all neighbors on the interface.

—

Step 15 **commit**

Configuring Authentication at Different Hierarchical Levels for OSPF Version 2

This task explains how to configure MD5 (secure) authentication on the OSPF router process, configure one area with plain text authentication, and then apply one interface with clear text (null) authentication.

Note Authentication configured at the interface level overrides authentication configured at the area level and the router process level. If an interface does not have authentication specifically configured, the interface inherits the authentication parameter value from a higher hierarchical level. See OSPF Hierarchical CLI and CLI Inheritance, on page 411 for more information about hierarchy and inheritance.

Before you begin

If you choose to configure authentication, you must first decide whether to configure plain text or MD5 authentication, and whether the authentication applies to all interfaces in a process, an entire area, or specific interfaces. See Route Authentication Methods for OSPF, on page 415 for information about each type of authentication and when you should use a specific method for your network.

Procedure

Step 1 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 2 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Step 3 **authentication** [**message-digest** | **null**]

Example:

```
RP/0/RP0:hostname(config-ospf)#authentication message-digest
```

Enables MD5 authentication for the OSPF process.

- This authentication type applies to the entire router process unless overridden by a lower hierarchical level such as the area or interface.

Step 4 **message-digest-key** *key-id* **md5** { *key* | **clear** *key* | **encrypted** *key* | **LINE**}

Example:

```
RP/0/RP0:hostname(config-ospf)#message-digest-key 4 md5 yourkey
```

Specifies the MD5 authentication key for the OSPF process.

- The neighbor routers must have the same key identifier.

Step 5 **area** *area-id*

Example:

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

Enters area configuration mode and configures a backbone area for the OSPF process.

Step 6 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/5.20
```

Enters interface configuration mode and associates one or more interfaces to the backbone area.

- All interfaces inherit the authentication parameter values specified for the OSPF process (Step 4, Step 5, and Step 6).

Step 7 Repeat Step 7 for each interface that must communicate, using the same authentication.

—

Step 8 **exit**

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# exit
```

Enters area OSPF configuration mode.

Step 9 **area** *area-id*

Example:

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

Enters area configuration mode and configures a nonbackbone area 1 for the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 10 **authentication** [**message-digest** | **null**]

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# authentication
```

Enables Type 1 (plain text) authentication that provides no security.

- The example specifies plain text authentication (by not specifying a keyword). Use the **authentication-key** command in interface configuration mode to specify the plain text password.

Step 11 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/3/0/9.21
```

Enters interface configuration mode and associates one or more interfaces to the nonbackbone area 1 specified in Step 7.

- All interfaces configured inherit the authentication parameter values configured for area 1.

Step 12 Repeat Step 12 for each interface that must communicate, using the same authentication.

—

Step 13 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to a different authentication type.

Step 14 **authentication** [**message-digest** | **null**]

Example:

```
RP/0/RP0:hostname(config-ospf-ar-if)# authentication null
```

Specifies no authentication on Ten Gigabit Ethernet interface 0/6/0/2.10, overriding the plain text authentication specified for area 1.

- By default, all of the interfaces configured in the same area inherit the same authentication parameter values of the area.

Step 15 **commit**

Controlling the Frequency That the Same LSA Is Originated or Accepted for OSPF

This task explains how to tune the convergence time of OSPF routes in the routing table when many LSAs need to be flooded in a very short time interval.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IP address as the router ID.

Step 4 Perform Step 5 or Step 6 or both to control the frequency that the same LSA is originated or accepted.

—

Step 5 **timers lsa refresh** *seconds*

Example:

```
RP/0/RP0:hostname(config-ospf)# timers lsa refresh 1800
```

Sets how often self-originated LSAs should be refreshed, in seconds.

- The default is 1800 seconds for both OSPF.

Step 6 **timers lsa min-arrival** *seconds*

Example:

```
RP/0/RP0:hostname(config-ospf)# timers lsa min-arrival 2
```

Limits the frequency that new processes of any particular OSPF Version 2 LSA can be accepted during flooding.

- The default is 1 second.

Step 7 **timers lsa group-pacing** *seconds*

Example:

```
RP/0/
/CPU0:router(config-ospf)# timers lsa group-pacing 1000
```

Changes the interval at which OSPF link-state LSAs are collected into a group for flooding.

- The default is 240 seconds.

Step 8 **commit**

Creating a Virtual Link with MD5 Authentication to Area 0 for OSPF

This task explains how to create a virtual link to your backbone (area 0) and apply MD5 authentication. You must perform the steps described on both ABRs, one at each end of the virtual link. To understand virtual links, see Virtual Link and Transit Area for OSPF, on page 420 .

Note After you explicitly configure area parameter values, they are inherited by all interfaces bound to that area—unless you override the values and configure them explicitly for the interface. An example is provided in Virtual Link Configured with MD5 Authentication for OSPF Version 2: Example, on page 473.

Before you begin

The following prerequisites must be met before creating a virtual link with MD5 authentication to area 0:

- You must have the router ID of the neighbor router at the opposite end of the link to configure the local router. You can execute the **show ospf** command on the remote router to get its router ID.
- For a virtual link to be successful, you need a stable router ID at each end of the virtual link. You do not want them to be subject to change, which could happen if they are assigned by default. (See OSPF Process and Router ID, on page 414 for an explanation of how the router ID is determined.) Therefore, we recommend that you perform one of the following tasks before configuring a virtual link:
  - Use the **router-id** command to set the router ID. This strategy is preferable.
  - Configure a loopback interface so that the router has a stable router ID.
- Before configuring your virtual link for OSPF Version 2, you must decide whether to configure plain text authentication, MD5 authentication, or no authentication (which is the default). Your decision determines whether you need to perform additional tasks related to authentication.

Note If you decide to configure plain text authentication or no authentication, see the **authentication** command provided in chapter *OSPF - IPv4 Commands on OTN and WDM Command Reference for Cisco NCS 4000 Series*

Procedure

Step 1 **show ospf** [*process-name*]

Example:

```
RP/0//CPU0:router# show ospf
```

(Optional) Displays general information about OSPF routing processes.

- The output displays the router ID of the local router. You need this router ID to configure the other end of the link.

Step 2 **configure**

Step 3 **router ospf** *process-name*

Example:

```
RP/0//CPU0:router(config)# router ospf 1
```

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 4 **router-id** { *router-id* }

Example:

```
RP/0//CPU0:router(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 5 **area** *area-id*

Example:

```
RP/0//CPU0:router(config-ospf)# area 1
```

Enters area configuration mode and configures a nonbackbone area for the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 6 **virtual-link** *router-id*

Example:

```
RRP/0//CPU0:router(config-ospf-ar)# virtual-link 10.3.4.5
```

Defines an OSPF virtual link.

- See .

Step 7 **authentication message-digest**

Example:

```
RP/0//CPU0:router(config-ospf-ar-vl)#authentication message-digest
```

Selects MD5 authentication for this virtual link.

Step 8 **message-digest-key** *key-id* **md5** { *key* | **clear** *key* | **encrypted** *key* }

Example:

```
RP/0//CPU0:router(config-ospf-ar-vl)#message-digest-key 4 md5 yourkey
```

Defines an OSPF virtual link.

- See to understand a virtual link.

- The *key-id* argument is a number in the range from 1 to 255. The *key* argument is an alphanumeric string of up to 16 characters. The routers at both ends of the virtual link must have the same key identifier and key to be able to route OSPF traffic.
- Once the key is encrypted it must remain encrypted.

Step 9 Repeat all of the steps in this task on the ABR that is at the other end of the virtual link. Specify the same key ID and key that you specified for the virtual link on this router.

—

Step 10 **commit**

Step 11 **show ospf** [*process-name*] [*area-id*] **virtual-links**

Example:

```
RP/0//CPU0:router# show ospf 1 2 virtual-links
```

(Optional) Displays the parameters and the current state of OSPF virtual links.

Summarizing Subnetwork LSAs on an OSPF ABR

If you configured two or more subnetworks when you assigned your IP addresses to your interfaces, you might want the software to summarize (aggregate) into a single LSA all of the subnetworks that the local area advertises to another area. Such summarization would reduce the number of LSAs and thereby conserve network resources. This summarization is known as interarea route summarization. It applies to routes from within the autonomous system. It does not apply to external routes injected into OSPF by way of redistribution.

This task configures OSPF to summarize subnetworks into one LSA, by specifying that all subnetworks that fall into a range are advertised together. This task is performed on an ABR only.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 4 **area** *area-id*

Example:

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

Enters area configuration mode and configures a nonbackbone area for the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 5 Do one of the following:

- **range** *ip-address mask* [**advertise** | **not-advertise**]
- **range** *ipv6-prefix* / *prefix-length* [**advertise** | **not-advertise**]

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# range 192.168.0.0 255.255.0.0 advertise
```

or

```
RP/0/RP0:hostname(config-ospf-ar)# range 4004:f000::/32 advertise
```

Consolidates and summarizes OSPF routes at an area boundary.

- The **advertise** keyword causes the software to advertise the address range of subnetworks in a Type 3 summary LSA.
- The **not-advertise** keyword causes the software to suppress the Type 3 summary LSA, and the subnetworks in the range remain hidden from other areas.
- In the first example, all subnetworks for network 192.168.0.0 are summarized and advertised by the ABR into areas outside the backbone.
- In the second example, two or more IPv4 interfaces are covered by a 192.*x.x* network.

Step 6 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 7 **commit**

Redistribute Routes into OSPF

This task redistributes routes from an IGP (could be a different OSPF process) into OSPF.

Before you begin

For information about configuring routing policy, see *Implementing Routing Policy on*

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RRP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 4 **redistribute** *protocol* [*process-id*] { **level-1** | **level-1-2** | **level-2** } [**metric** *metric-value*] [**metric-type** *type-value*] [**match** { **external** [**1** | **2**]} [**tag** *tag-value*] [**route-policy** *policy-name*]

Example:

```
RP/0/RP0:hostname(config-ospf)# redistribute bgp 100
```

or

```
RP/0/RP0:hostname(config-router)#redistribute bgp 110
```

Redistributes OSPF routes from one routing domain to another routing domain.

- This command causes the router to become an ASBR by definition.
- OSPF tags all routes learned through redistribution as external.
- The protocol and its process ID, if it has one, indicate the protocol being redistributed into OSPF.
- The metric is the cost you assign to the external route. The default is 20 for all protocols except BGP, whose default metric is 1.
- The OSPF example redistributes BGP autonomous system 1, Level 1 routes into OSPF as Type 2 external routes.

Step 5 Do one of the following:

- **summary-prefix** *address* *mask* [**not-advertise**] [**tag** *tag*]
- **summary-prefix** *ipv6-prefix* / *prefix-length* [**not-advertise**] [**tag** *tag*]

Example:

```
RP/0/RP0:hostname(config-ospf)# summary-prefix 10.1.0.0 255.255.0.0
```

or

```
RP/0/RP0:hostname(config-router)# summary-prefix 2010:11:22::/32
```

(Optional) Creates aggregate addresses for OSPF.

- This command provides external route summarization of the non-OSPF routes.
- External ranges that are being summarized should be contiguous. Summarization of overlapping ranges from two different routers could cause packets to be sent to the wrong destination.
- This command is optional. If you do not specify it, each route is included in the link-state database and advertised in LSAs.
- In the OSPFv2 example, the 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 LSA.

Step 6 **commit**

Configuring OSPF Shortest Path First Throttling

This task explains how to configure SPF scheduling in millisecond intervals and potentially delay SPF calculations during times of network instability. This task is optional.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 4 **timers throttle spf** *spf-start spf-hold spf-max-wait*

Example:

```
RP/0/RP0:hostname(config-ospf)# timers throttle spf 10 4800 90000
```

Sets SPF throttling timers.

Step 5 **area** *area-id*

Example:

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

Enters area configuration mode and configures a backbone area.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 6 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 7 **commit**

Step 8 **show ospf** [*process-name*]

Example:

```
RP/0/RP0:hostname# show ospf 1
```

(Optional) Displays SPF throttling timers.

Examples

In the following example, the **show ospf** XR EXEC command is used to verify that the initial SPF schedule delay time, minimum hold time, and maximum wait time are configured correctly. Additional details are displayed about the OSPF process, such as the router type and redistribution of routes.

```
show ospf 1

 Routing Process "ospf 1" with ID 192.168.4.3
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  It is an autonomous system boundary router
  Redistributing External Routes from,
     ospf 2
  Initial SPF schedule delay 5 msecs
  Minimum hold time between two consecutive SPFs 100 msecs
  Maximum wait time between two consecutive SPFs 1000 msecs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  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 1. 1 normal 0 stub 0 nssa
```

```
External flood list length 0
Non-Stop Forwarding enabled
```

Note For a description of each output display field, see the **show ospf** command in the *OSPF-IPv4 Commands on OTN and WDM Command Reference for Cisco NCS 4000 Series*

Configuring Nonstop Forwarding Specific to Cisco for OSPF Version 2

This task explains how to configure OSPF NSF specific to Cisco on your NSF-capable router. This task is optional.

Before you begin

OSPF NSF requires that all neighbor networking devices be NSF aware, which happens automatically after you install the Cisco IOS XR software image on the router. If an NSF-capable router discovers that it has non-NSF-aware neighbors on a particular network segment, it disables NSF capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware routers continue to provide NSF capabilities.

Note The following are restrictions when configuring nonstop forwarding:

- OSPF Cisco NSF for virtual links is not supported.
- Neighbors must be NSF aware.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 4 Do one of the following:

- **nsf cisco**
- **nsf cisco enforce global**

Example:

```
RP/0/RP0:hostname(config-ospf)# nsf cisco enforce global
```

Enables Cisco NSF operations for the OSPF process.

- Use the **nsf cisco** command without the optional **enforce** and **global** keywords to terminate the NSF restart mechanism on the interfaces of detected non-NSF neighbors and allow NSF neighbors to function properly.
- Use the **nsf cisco** command with the optional **enforce** and **global** keywords if the router is expected to perform NSF during restart. However, if non-NSF neighbors are detected, NSF restart is canceled for the entire OSPF process.

Step 5 **nsf interval** *seconds*

Example:

```
RP/0/RP0:hostname(config-ospf)# nsf interval 120
```

Sets the minimum time between NSF restart attempts.

Note When you use this command, the OSPF process must be up for at least 90 seconds before OSPF attempts to perform an NSF restart.

Step 6 **nsfflush-delay-time***seconds*

Example:

```
RP/0/RP0:hostname(config-ospf)#nsf flush-delay-time 1000
```

Sets the maximum time allowed for external route learning in seconds.

Step 7 **nsflifetime***seconds*

Example:

```
RP/0/RP0:hostname(config-ospf)#nsf lifetime 90
```

Sets the maximum route lifetime of NSF following a restart in seconds.

Step 8 **nsfietf**

Example:

```
RP/0/RP0:hostname(config-ospf)#nsf ietf
```

Enables ietf graceful restart.

Step 9 **commit**

Configuring OSPF Version 2 for MPLS Traffic Engineering

This task explains how to configure OSPF for MPLS TE. This task is optional.

Before you begin

Your network must support the following features before you enable MPLS TE for OSPF on your router:

- MPLS
- IP Cisco Express Forwarding (CEF)

Note You must enter the commands in the following task on every OSPF router in the traffic-engineered portion of your network.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 4 **mpls traffic-eng router-id** *interface-type interface-instance*

Example:

```
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng router-id loopback 0
```

(Optional) Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.

- This IP address is flooded to all nodes in TE LSAs.
- 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.

- We recommend that loopback interfaces be used for MPLS TE router ID because they are more stable than physical interfaces.

Step 5 **area** *area-id*

Example:

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

Enters area configuration mode and configures an area for the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area.

Step 6 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng
```

Configures the MPLS TE under the OSPF area.

Step 7 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface interface loopback0
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 8 **commit**

Step 9 **show ospf** [*process-name*] [*area-id*] **mpls traffic-eng** { **link** | **fragment** }

Example:

```
RP/0/RP0:hostname# show ospf 1 0 mpls traffic-eng link
```

(Optional) Displays information about the links and fragments available on the local router for MPLS TE.

Examples

This section provides the following output examples:

Sample Output for the show ospf Command Before Configuring MPLS TE

In the following example, the **show route ospf** XR EXEC command verifies that Ten Gigabit Ethernet interface 0/6/0/2.10 exists and MPLS TE is not configured:

```
show route ospf 1

 O    11.0.0.0/24 [110/15] via 0.0.0.0, 3d19h, tunnel-te1
 O    192.168.0.12/32 [110/11] via 11.1.0.2, 3d19h, TenGigE0/6/0/2.10
 O    192.168.0.13/32 [110/6] via 0.0.0.0, 3d19h, tunnel-te1
```

Sample Output for the show ospf mpls traffic-eng Command

In the following example, the **show ospf mpls traffic-eng** XR EXEC command verifies that the MPLS TE fragments are configured correctly:

```
 show ospf 1 mpls traffic-eng fragment

OSPF Router with ID (192.168.4.3) (Process ID 1)

  Area 0 has 1  MPLS TE fragment. Area instance is 3.
  MPLS router address is 192.168.4.2
  Next fragment ID is 1

  Fragment 0 has 1 link. Fragment instance is 3.
  Fragment has 0 link the same as last update.
  Fragment advertise MPLS router address
    Link is associated with fragment 0. Link instance is 3
      Link connected to Point-to-Point network
      Link ID :55.55.55.55
      Interface Address :192.168.50.21
      Neighbor Address :192.168.4.1
      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
```

In the following example, the **show ospf mpls traffic-eng** XR EXEC command verifies that the MPLS TE links on area instance 3 are configured correctly:

```
show ospf mpls traffic-eng link

             OSPF Router with ID (192.168.4.1) (Process ID 1)

   Area 0 has 1  MPLS TE links. Area instance is 3.

   Links in hash bucket 53.
     Link is associated with fragment 0. Link instance is 3
       Link connected to Point-to-Point network
       Link ID :192.168.50.20
       Interface Address :192.168.20.50
       Neighbor Address :192.168.4.1
       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
```

Sample Output for the show ospf Command After Configuring MPLS TE

In the following example, the **show route ospf** XR EXEC command verifies that the MPLS TE tunnels replaced Ten Gigabit Ethernet interface 0/6/0/2.10 and that configuration was performed correctly:

```
show route ospf 1

 O E2 192.168.10.0/24 [110/20] via 0.0.0.0, 00:00:15, tunnel2
 O E2 192.168.11.0/24 [110/20] via 0.0.0.0, 00:00:15, tunnel2
 O E2 192.168.1244.0/24 [110/20] via 0.0.0.0, 00:00:15, tunnel2
 O    192.168.12.0/24 [110/2] via 0.0.0.0, 00:00:15, tunnel2
```

Enabling Nonstop Routing for OSPFv2

This optional task describes how to enable nonstop routing (NSR) for OSPFv2 process. NSR is disabled by default. When NSR is enabled, OSPF process on the active RP synchronizes all necessary data and states with the OSPF process on the standby RP. When the switchover happens, 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.

Procedure

Step 1 **configure**

Enter the global configuration mode.

Step 2 **router ospf** *instance-id*

Example:

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

Enable OSPF routing for the specified routing process. In this example, the OSPF instance is called isp.

Step 3 **nsr**

Example:

```
RP/0/RP0:hostname(config-ospf)# nsr
```

Enable NSR for the OSPFv2 process.

Step 4 **commit**

Commit your configuration.

Configuring OSPFv2 OSPF SPF Prefix Prioritization

Perform this task to configure OSPFv2 OSPF SPF (shortest path first) prefix prioritization.

Procedure

Step 1 **configure**

Step 2 **prefix-set** *prefix-set name*

Example:

```
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
```

Configures the prefix set.

Step 3 **route-policy** *route-policy name* **if destination in** *prefix-set name* **then set spf-priority** {**critical** | **high** | **medium**} **endif**

Example:

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

Configures route policy and sets OSPF SPF priority.

Step 4 **router ospf** *ospf-name*

Example:

```
RP/0/RP0:hostname# router ospf 1
```

Enters Router OSPF configuration mode.

Step 5 **router ospf** *ospf name*

Example:

```
RP/0/RP0:hostname# router ospf 1
```

Enters Router OSPF configuration mode.

Step 6 **spf prefix-priority route-policy** *route-policy name*

Example:

```
RP/0/RP0:hostname(config-ospf)# spf prefix-priority route-policy ospf-spf-priority
```

Configures SPF prefix-priority for the defined route policy.

Note Configure the **spf prefix-priority** command under router OSPF.

Step 7 **commit**

Step 8 **show rpl route-policy** *route-policy name* **detail**

Example:

```
RP/0/RP0:hostname#show rpl route-policy ospf-spf-priority detail
  prefix-set ospf-critical-prefixes
    66.0.0.0/16
  end-set
  !
  route-policy ospf-spf-priority
    if destination in ospf-critical-prefixes then
      set spf-priority critical
    endif
  end-policy
  !
```

Displays the set SPF prefix priority.

Enabling Multicast-intact for OSPFv2

This optional task describes how to enable multicast-intact for OSPFv2 routes that use IPv4 addresses.

Procedure

Step 1 **configure**

Step 2 **router ospf** *instance-id*

Example:

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

Enables OSPF routing for the specified routing process, and places the router in router configuration mode. In this example, the OSPF instance is called isp.

Step 3 **mpls traffic-eng multicast-intact**

Example:

```
RP/0/RP0:hostname(config-ospf)# mpls traffic-eng multicast-intact
```

Enables multicast-intact.

Step 4 **commit**

Associating Interfaces to a VRF

This task explains how to associate an interface with a VPN Routing and Forwarding (VRF) instance.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RP0:hostname(config-ospf)# vrf vrf1
```

Creates a VRF instance and enters VRF configuration mode.

Step 4 **area** *area-id*

Example:

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

Enters area configuration mode and configures an area for the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area.

Step 5 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-vrf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the VRF.

Step 6 **commit**

Configuring OSPF as a Provider Edge to Customer Edge (PE-CE) Protocol

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RP0:hostname(config-ospf)# vrf vrf1
```

Creates a VRF instance and enters VRF configuration mode.

Step 4 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf-vrf)# router-id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 5 **redistribute** *protocol* [*process-id*] { **level-1** | **level-1-2** | **level-2** } [**metric** *metric-value*] [**metric-type** *type-value*] [**match** { **external** [**1** | **2**] }] [**tag** *tag-value*] **route-policy** *policy-name*]

Example:

```
RP/0/RP0:hostname(config-ospf-vrf)# redistribute bgp 1 level-1
```

Redistributes OSPF routes from one routing domain to another routing domain.

- This command causes the router to become an ASBR by definition.
- OSPF tags all routes learned through redistribution as external.
- The protocol and its process ID, if it has one, indicate the protocol being redistributed into OSPF.
- The metric is the cost you assign to the external route. The default is 20 for all protocols except BGP, whose default metric is 1.
- The example shows the redistribution of BGP autonomous system 1, Level 1 routes into OSPF as Type 2 external routes.

Step 6 **area** *area-id*

Example:

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

Enters area configuration mode and configures an area for the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area.

Step 7 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-vrf)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the VRF.

Step 8 exit

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration mode.

Step 9 **domain-id** *[* **secondary** *]* **type** *{* **0005** | **0105** | **0205** | **8005** *}* **value** *value*

Example:

```
RP/0/RP0:hostname(config-ospf-vrf)# domain-id type 0105 value 1AF234
```

Specifies the OSPF VRF domain ID.

- The *value* argument is a six-octet hex number.

Step 10 **domain-tag** *tag*

Example:

```
RP/0/RP0:hostname(config-0spf-vrf)# domain-tag 234
```

Specifies the OSPF VRF domain tag.

- The valid range for *tag* is 0 to 4294967295.

Step 11 disable-dn-bit-check

Example:

```
RP/0/RP0:hostname(config-ospf-vrf)# disable-dn-bit-check
```

Specifies that down bits should be ignored.

Step 12 **commit**

Creating Multiple OSPF Instances (OSPF Process and a VRF)

This task explains how to create multiple OSPF instances. In this case, the instances are a normal OSPF instance and a VRF instance.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **area** *area-id*

Example:

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

Enters area configuration mode and configures a backbone area.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 5 **exit**

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# exit
```

Enters OSPF configuration mode.

Step 6 **vrf** *vrf-name*

Example:

```
RP/0/RP0:hostname(config-ospf)# vrf vrf1
```

Creates a VRF instance and enters VRF configuration mode.

Step 7 **area** *area-id*

Example:

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

Enters area configuration mode and configures an area for a VRF instance under the OSPF process.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area.

Step 8 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-vrf)# interface TenGigE0/3/0/5.20
```

Enters interface configuration mode and associates one or more interfaces to the VRF.

Step 9 **commit**

Configuring Multi-area Adjacency

This task explains how to create multiple areas on an OSPF primary interface.

Before you begin

Note 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.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **area** *area-id*

Example:

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

Enters area configuration mode and configures a backbone area.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface Serial 0/1/0/3
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 5 **area** *area-id*

Example:

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

Enters area configuration mode and configures an area used for multiple area adjacency.

- The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 6 **multi-area-interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf)# multi-area-interface Serial 0/1/0/3
```

Enables multiple adjacencies for different OSPF areas and enters multi-area interface configuration mode

Step 7 **commit**

Configuring Authentication Message Digest Management for OSPF

This task explains how to manage authentication of a keychain on the OSPF interface.

Before you begin

A valid keychain must be configured before this task can be attempted.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router id 192.168.4.3
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 4 **area** *area-id*

Example:

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

Enters area configuration mode.

The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 5 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 6 **authentication message-digest keychain** *keychain*

Example:

```
RP/0/RP0:hostname(config-ospf-ar-if)# authentication message-digest keychain ospf_int1
```

Configures an MD5 keychain.

Note In the example, the *ospf_intl* keychain must be configured before you attempt this step.

Step 7 **commit**

Examples

The following example shows how to configure the keychain *ospf_intf_1* that contains five key IDs. Each key ID is configured with different **send-lifetime** values; however, all key IDs specify the same text string for the key.

```
key chain ospf_intf_1
key 1
send-lifetime 11:30:30 May 1 2007 duration 600
cryptographic-algorithm MD5T
key-string clear ospf_intf_1
key 2
send-lifetime 11:40:30 May 1 2007 duration 600
cryptographic-algorithm MD5
key-string clear ospf_intf_1
key 3
send-lifetime 11:50:30 May 1 2007 duration 600
cryptographic-algorithm MD5
key-string clear ospf_intf_1
key 4
send-lifetime 12:00:30 May 1 2007 duration 600
cryptographic-algorithm MD5
key-string clear ospf_intf_1
key 5
send-lifetime 12:10:30 May 1 2007 duration 600
cryptographic-algorithm MD5
key-string clear ospf_intf_1
```

The following example shows that keychain authentication is enabled on the TenGigE0/6/0/2.10 interface:

```
show ospf 1 interface TenGigE0/3/0/5.20
```

```
TenGigE0/3/0/5.20 is up, line protocol is up
  Internet Address 100.10.10.2/24, Area 0
  Process ID 1, Router ID 2.2.2.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.1, Interface address 100.10.10.2
  Backup Designated router (ID) 1.1.1.1, Interface address 100.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 3/3, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 2, maximum is 16
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Keychain-based authentication enabled
    Key id used is 3
  Multi-area interface Count is 0
```

The following example shows output for configured keys that are active:

```
show key chain ospf_intf_1

 Key-chain: ospf_intf_1/ -

 Key 1 -- text "0700325C4836100B0314345D"
   cryptographic-algorithm -- MD5
   Send lifetime:   11:30:30, 01 May 2007 - (Duration) 600
   Accept lifetime: Not configured
 Key 2 -- text "10411A0903281B051802157A"
   cryptographic-algorithm -- MD5
   Send lifetime:   11:40:30, 01 May 2007 - (Duration) 600
   Accept lifetime: Not configured
 Key 3 -- text "06091C314A71001711112D5A"
   cryptographic-algorithm -- MD5
   Send lifetime:   11:50:30, 01 May 2007 - (Duration) 600  [Valid now]
   Accept lifetime: Not configured
 Key 4 -- text "151D181C0215222A3C350A73"
   cryptographic-algorithm -- MD5
   Send lifetime:   12:00:30, 01 May 2007 - (Duration) 600
   Accept lifetime: Not configured
 Key 5 -- text "151D181C0215222A3C350A73"
   cryptographic-algorithm -- MD5
   Send lifetime:   12:10:30, 01 May 2007 - (Duration) 600
   Accept lifetime: Not configured
```

Configuring Generalized TTL Security Mechanism (GTSM) for OSPF

This task explains how to set the security time-to-live mechanism on an interface for GTSM.

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Note The *process-name* argument is any alphanumeric string no longer than 40 characters.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RP0:hostname(config-ospf)# router id 10.10.10.100
```

Configures a router ID for the OSPF process.

Note We recommend using a stable IPv4 address as the router ID.

Step 4 **log adjacency changes** [**detail** | **disable**]

Example:

```
RP/0/RP0:hostname(config-ospf-ar-if)# log adjacency changes detail
```

(Optional) Requests notification of neighbor changes.

- By default, this feature is enabled.
- The messages generated by neighbor changes are considered notifications, which are categorized as severity Level 5 in the **logging console** command. The **logging console** command controls which severity level of messages are sent to the console. By default, all severity level messages are sent.

Step 5 **nsf** { **cisco** [**enforce global**] | **ietf** [**helper disable**]}

Example:

```
RP/0/RP0:hostname(config-ospf)# nsf ietf
```

(Optional) Configures NSF OSPF protocol.

The example enables graceful restart.

Step 6 **timers throttle spf** *spf-start spf-hold spf-max-wait*

Example:

```
RP/0/RP0:hostname(config-ospf)# timers throttle spf 500 500 10000
```

(Optional) Sets SPF throttling timers.

Step 7 **area** *area-id*

Example:

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

Enters area configuration mode.

The *area-id* argument can be entered in dotted-decimal or IPv4 address notation, such as area 1000 or area 0.0.3.232. However, you must choose one form or the other for an area. We recommend using the IPv4 address notation.

Step 8 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 9 **security ttl** [**disable** | **hops** *hop-count*]

Example:

```
RP/0/RP0:hostname(config-ospf-ar-if)# security ttl hopes 2
```

Sets the security TTL value in the IP header for OSPF packets.

Step 10 **commit**

Step 11 **show ospf** [*process-name*] [*area-id*] **interface** [*type interface-path-id*]

Example:

```
RP/0/RP0:hostname# show ospf 1 interface TenGigE0/6/0/2.10
```

Displays OSPF interface information.

Examples

The following is sample output that displays the GTSM security TTL value configured on an OSPF interface:

```
 show ospf 1 interface TenGigE0/6/0/2.10

  TenGigE0/6/0/2.10 is up, line protocol is up
    Internet Address 120.10.10.1/24, Area 0
    Process ID 1, Router ID 100.100.100.100, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State BDR, Priority 1
    TTL security enabled, hop count 2
    Designated Router (ID) 102.102.102.102, Interface address 120.10.10.3
    Backup Designated router (ID) 100.100.100.100, Interface address 120.10.10.1
    Flush timer for old DR LSA due in 00:02:36
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:05
    Index 1/1, flood queue length 0
    Next 0(0)/0(0)
    Last flood scan length is 1, maximum is 4
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1, Adjacent neighbor count is 1
      Adjacent with neighbor 102.102.102.102  (Designated Router)
    Suppress hello for 0 neighbor(s)
    Multi-area interface Count is 0
```

Verifying OSPF Configuration and Operation

This task explains how to verify the configuration and operation of OSPF.

Procedure

Step 1 **show** { **ospf** } [*process-name*]

Example:

```
RP/0/RP0:hostname# show ospf group1
```

(Optional) Displays general information about OSPF routing processes.

Step 2 **show** { **ospf** } [*process-name*] **border-routers** [*router-id*]

Example:

```
RP/0/RP0:hostname# show ospf group1 border-routers
```

(Optional) Displays the internal OSPF routing table entries to an ABR and ASBR.

Step 3 **show** { **ospf** } [*process-name*] **database**

Example:

```
RP/0/RP0:hostname# show ospf group2 database
```

(Optional) Displays the lists of information related to the OSPF database for a specific router.

- The various forms of this command deliver information about different OSPF LSAs.

Step 4 **show** { **ospf** } [*process-name*] [*area-id*] **flood-list interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname# show ospf 100 flood-list interface TenGigE0/6/0/2.10
```

(Optional) Displays a list of OSPF LSAs waiting to be flooded over an interface.

Step 5 **show** { **ospf** } [*process-name*] [*area-id*] **interface** [*type interface-path-id*]

Example:

```
RP/0/RP0:hostname# show ospf 100 interface TenGigE0/6/0/2.10
```

(Optional) Displays OSPF interface information.

Step 6 **show** { **ospf** }[*process-name*] [*area-id*] **neighbor** [*t ype interface- path-id*] [*neighbor-id*] [**detail**]

Example:

```
RP/0/RP0:hostname# show ospf 100 neighbor
```

(Optional) Displays OSPF neighbor information on an individual interface basis.

Step 7 **clear** { **ospf** }[*process-name*] **process**

Example:

```
RP/0/
/CPU0:router# clear ospf 100 process
```

(Optional) Resets an OSPF router process without stopping and restarting it.

Step 8 **clear**{**ospf**[*process-name*] **redistribution**

Example:

```
RP/0/RP0:hostname#clear ospf 100 redistribution
```

Clears OSPF route redistribution.

Step 9 **clear**{**ospf**[*process-name*] **routes**

Example:

```
RP/0/RP0:hostname#clear ospf 100 routes
```

Clears OSPF route table.

Step 10 **clear**{**ospf**[*process-name*] **vrf** [*vrf-name*|**all**] {**process** |**redistribution**|**routes**|**statistics** [**interface** *type interface-path-id*|**message-queue**|**neighbor**]}

Example:

```
RP/0/RP0:hostname#clear ospf 100 vrf vrf_1 process
```

Clears OSPF route table.

Step 11 **clear** { **ospf** }[*process-name*] **statistics** [**neighbor** [*type interface-path-id*] [*ip-address*]]

Example:

```
RP/0/RP0:hostname# clear ospf 100 statistics
```

(Optional) Clears the OSPF statistics of neighbor state transitions.

Configuring IP Fast Reroute Loop-free Alternate

This task describes how to enable the IP fast reroute (IPFRR) per-link loop-free alternate (LFA) computation to converge traffic flows around link failures.

To enable protection on broadcast links, IPFRR and bidirectional forwarding detection (BFD) must be enabled on the interface under OSPF.

Enabling IPFRR LFA

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Step 3 **area** *area-id*

Example:

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

Enters area configuration mode.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)#  interface TenGigE0/6/0/2.10
```

Enters interface configuration mode and associates one or more interfaces to the area. .

Step 5 **fast-reroute per-link** { **enable** | **disable** }

Example:

```
RP/0/RP0:hostname(config-ospf-ar)#fast-reroute per-link enable
```

Enables or disables per-link LFA computation for the interface.

Step 6 **commit**

Excluding an Interface From IP Fast Reroute Per-link Computation

Procedure

Step 1 **configure**

Step 2 **router ospf** *process-name*

Example:

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

Enables the OSPF routing for the specified routing process and places the router in router configuration mode.

Step 3 **area** *area-id*

Example:

```
RP/0/RP0:hostname(config)#area area-id
```

Enters area configuration mode.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf)#interface type interface-path-id
```

Enters interface configuration mode and associates one or more interfaces to the area.

Step 5 **fast-reroute per-link exclude interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-ospf-ar)# fast-reroute per-link exclude interface TenGigE0/6/0/2.10
```

Excludes an interface from IP fast reroute per-link computation.

Step 6 **commit**

Enabling OSPF Interaction with SRMS Server

To enable OSPF interaction with SRMS server:

Procedure

Step 1 **configure**

Step 2 **router ospf** *instance-id*

Example:

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

Enables OSPF routing for the specified routing instance, and places the router in router configuration mode.

Step 3 **segment-routing mpls**

Example:

```
RP/0/RP0:hostname(config-ospf)# segment-routing mpls
```

Step 4 **segment-routing forwarding mpls**

Example:

```
RP/0/RP0:hostname(config-ospf)# segment-routing forwarding mpls
```

Enables SR forwarding on all interfaces where this instance OSPF is enabled.

Step 5 **segment-routing prefix-sid-mapadvertise-local**

Example:

```
RP/0/RP0:hostname(config-ospf)# segment-routing
prefix-sid-map advertise local
```

Enables server functionality and allows OSPF to advertise the local mapping entries using area-scope flooding. The flooding is limited to areas where segment-routing is enabled. Disabled by default.

Step 6 **segment-routing sr-preferprefix-list***[acl-name]*

Example:

```
RP/0/RP0:hostname(config-ospf)# segment-routing
 sr-prefer prefix-list foo
```

Configuration Examples for Implementing OSPF

This section provides the following configuration examples:

Cisco IOS XR Software for OSPF Version 2 Configuration: Example

The following example shows how an OSPF interface is configured for an area in Cisco IOS XR Software.

area 0 must be explicitly configured with the **area** command and all interfaces that are in the range from 10.1.2.0 to 10.1.2.255 are bound to area 0. Interfaces are configured with the **interface** command (while the router is in area configuration mode) and the **area** keyword is not included in the interface statement.

Cisco IOS XR Software Configuration

```
interface TenGigE0/3/0/2.10
 ip address 10.1.2.1 255.255.255.255
 negotiation auto
!
router ospf 1
router-id 10.2.3.4
 area 0
  interface TenGigE0/3/0/2.10
!
!
```

The following example shows how OSPF interface parameters are configured for an area in Cisco IOS XR software.

In Cisco IOS XR software, OSPF interface-specific parameters are configured in interface configuration mode and explicitly defined for area 0. In addition, the **ip ospf** keywords are no longer required.

Cisco IOS XR Software Configuration

```
interface TenGigE0/3/0/2.10
 ip address 10.1.2.1 255.255.255.0
 negotiation auto
!
router ospf 1
 router-id 10.2.3.4
area 0
 interface TenGigE0/3/0/2.10
  cost 77
  mtu-ignore
  authentication message-digest
  message-digest-key 1 md5 0 test
!
!
```

The following example shows the hierarchical CLI structure of Cisco IOS XR software:

In Cisco IOS XR software, OSPF areas must be explicitly configured, and interfaces configured under the area configuration mode are explicitly bound to that area. In this example, interface 10.1.2.0/24 is bound to area 0 and interface 10.1.3.0/24 is bound to area 1.

Cisco IOS XR Software Configuration

```
interface TenGigE0/3/0/2.10
 ip address 10.1.2.1 255.255.255.0
 negotiation auto
!
interface TenGigE0/3/0/5.20
 ip address 10.1.3.1 255.255.255.0
 negotiation auto
```

```
!
router ospf 1
 router-id 10.2.3.4
area 0
 interface TenGigE0/3/0/2.10
!
area 1
 interface TenGigE0/3/0/5.20
!
!
```

MPLS TE for OSPF Version 2: Example

The following example shows how to configure the OSPF portion of MPLS TE. However, you still need to build an MPLS TE topology and create an MPLS TE tunnel.

In this example, loopback interface 0 is associated with area 0 and MPLS TE is configured within area 0.

```
interface Loopback 0
 address 10.10.10.10 255.255.255.0
!
interface TenGigE0/3/0/2.10
 address 10.1.2.2 255.255.255.0
!
router ospf 1
 router-id 10.10.10.10
 nsf
 auto-cost reference-bandwidth 10000
 mpls traffic-eng router-id Loopback 0
 area 0
  mpls traffic-eng
  interface TenGigE0/3/0/2.10
  interface Loopback 0
```

Virtual Link Configured with MD5 Authentication for OSPF Version 2: Example

The following examples show how to configure a virtual link to your backbone and apply MD5 authentication. You must perform the steps described on both ABRs at each end of the virtual link.

After you explicitly configure the ABRs, the configuration is inherited by all interfaces bound to that area—unless you override the values and configure them explicitly for the interface.

To understand virtual links, see Virtual Link and Transit Area for OSPF, on page 420.

In this example, all interfaces on router ABR1 use MD5 authentication:

```
router ospf ABR1
 router-id 10.10.10.10
 authentication message-digest
 message-digest-key 100 md5 0 cisco
 area 0
  interface TenGigE0/3/0/2.10
  interface TenGigE0/6/0/5.20
 area 1
  interface TenGigE0/14/0/4.40
  virtual-link 10.10.5.5
!
!
```

In this example, only area 1 interfaces on router ABR3 use MD5 authentication:

```
router ospf ABR2
 router-id 10.10.5.5
 area 0
 area 1
  authentication message-digest
  message-digest-key 100 md5 0 cisco
  interface TenGigE0/3/0/5.20
  virtual-link 10.10.10.10
 area 3
  interface Loopback 0
  interface TenGigE0/3/0/2.10
!
```

CHAPTER 39

Configure Ethernet OAM

This chapter describes the Cisco IOS XR commands to configure Ethernet OAM.

Table 37: Feature History

Feature Name	Release Information	Feature Description
Delay Measurement	Cisco IOS XR Release 6.5.31	This feature supports hardware timestamping for both one-way and two-way delay measurements. The delay measurement can be performed only after the Precision Time Protocol (PTP) is configured and the clocks are in sync. The delay measurement packets contain timestamps within the packet data that can be used to accurately measureframe delay, jitter, and round-trip statistics.

Understanding PTP

Precision Time Protocol (PTP) is a protocol that defines a method to distribute time around a network. PTP support is based on the IEEE 1588-2008 standard. PTP synchronizes with the real-time clocks of the devices in a network at nanosecond accuracy. The clocks are organized into a primary-secondary hierarchy. PTP identifies the port that is connected to a device with the most precise clock. This clock is referred to as the primary clock. All the other devices on the network synchronize their clocks with the primary clock and are referred to as members. Constantly exchanged timing messages ensure continued synchronization.

Note When PTP switching happens between interfaces, internal servo status might move to Freerun and restore to PHASE_LOCKED state. This is expected in NCS 4000.

ITU-T Telecom Profiles for PTP

Cisco IOS XR software supports ITU-T Telecom Profiles for PTP as defined in the ITU-T recommendations. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application.

PTP lets you define separate profiles to adapt itself for use in different scenarios. A telecom profile differs in several ways from the default behavior defined in the IEEE 1588-2008 standard.

G.8275.1 ITU-T telecom profile is supported for PTP.

G.8275.1

G.8275.1 profile fulfills the time-of-day and phase synchronization requirements in telecom networks with all network devices participating in the PTP protocol. G.8275.1 profile provides better frequency stability for the time-of-day and phase synchronization.

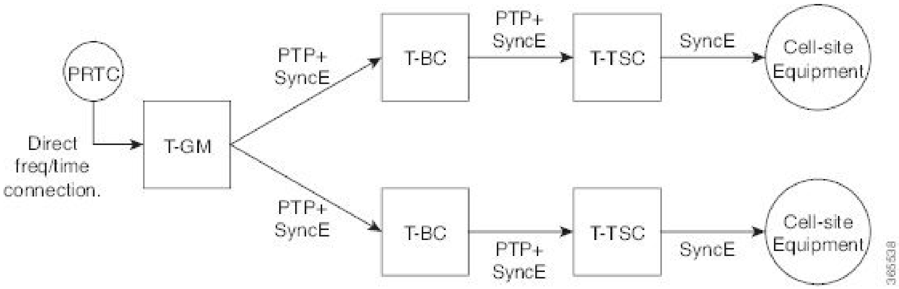
Features of G.8275.1 profile are:

- Synchronization Model: G.8275.1 profile adopts hop-by-hop synchronization model. Each network device in the path from primary to secondary synchronizes its local clock to upstream devices and provides synchronization to downstream devices.
- Clock Selection: G.8275.1 profile also defines an alternate BMCA that selects a clock for synchronization and port state for the local ports of all devices in the network is defined for the profile. The parameters defined as a part of the BMCA are:
  - Clock Class
  - Clock Accuracy
  - Offset Scaled Log Variance
  - Priority 2
  - Clock Identity
  - Steps Removed
  - Port Identity
  - notSlave flag
  - Local Priority
- Port State Decision: The port states are selected based on the alternate BMCA algorithm. A port is configured to a primary-only port state to enforce the port to be a primary for multicast transport mode.
- Packet Rates: The nominal packet rate for Announce packets is 8 packets-per-second and 16 packets-per-second for Sync/Follow-Up and Delay-Request/Delay-Response packets.
- Transport Mechanism: G.8275.1 profile supports only Ethernet PTP transport mechanism.

- Mode: G.8275.1 profile supports transport of data packets only in multicast mode. The forwarding is done based on forwardable or non-forwardable multicast MAC address.
- Domain Numbers: The domain numbers that can be used in a G.8275.1 profile network ranges from 24 to 43. The default domain number is 24.
- Clock Type: G.8275.1 profile supports the following clock types:
  - T-GM: The telecom grandmaster (T-GM) provides timing to all other devices on the network. It does not synchronize its local clock with any other network element other than the Primary Reference Time Clock (PRTC).
  - T-BC: The telecom boundary clock (T-BC) synchronizes its local clock to a T-GM or an upstream T-BC and provides timing information to downstream T-BCs or T-TSCs. If at a given point in time there are no higher-quality clocks available to a T-BC to synchronize to, it may act as a grandmaster.
  - T-TSC: The telecom time slave clock (T-TSC) synchronizes its local clock to another PTP clock (in most cases, the T-BC), and does not provide synchronization through PTP to any other device.

The following figure describes a sample G.8275.1 topology.

Figure 16: A Sample G.8275.1 Topology



Configuring Global G.8275.1 Profile

The following configuration describes the steps involved to create a global configuration profile for a PTP interface that can then be assigned to any interface as required. It uses G.8275.1 profile as an example

Procedure

Example:

```
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
RP/0/RP0/CPU0:router(config-ptp)# profile slave
RP/0/RP0/CPU0:router(config-ptp-profile)# multicast target-address ethernet 01-1B-19-00-00-00
RP/0/RP0/CPU0:router(config-ptp-profile)# transport ethernet
RP/0/RP0/CPU0:router(config-ptp-profile)# sync frequency 16
RP/0/RP0/CPU0:router(config-ptp-profile)# announce frequency 8
RP/0/RP0/CPU0:router(config-ptp-profile)# delay-request frequency 16
```

```
RP/0/RP0/CPU0:router(config-ptp-profile)# exit
RP/0/RP0/CPU0:router(config-ptp)# profile master
RP/0/RP0/CPU0:router(config-ptp-profile)# multicast target-address ethernet 01-1B-19-00-00-00
RP/0/RP0/CPU0:router(config-ptp-profile)# transport ethernet
RP/0/RP0/CPU0:router(config-ptp-profile)# sync frequency 16
RP/0/RP0/CPU0:router(config-ptp-profile)# announce frequency 8
RP/0/RP0/CPU0:router(config-ptp-profile)# delay-request frequency 16
RP/0/RP0/CPU0:router(config-ptp-profile)# exit
RP/0/RP0/CPU0:router(config-ptp)# physical-layer-frequency
RP/0/RP0/CPU0:router(config-ptp)# log
RP/0/RP0/CPU0:router(config-ptp-log)# servo events
RP/0/RP0/CPU0:router(config-ptp-log)# commit
```

Configuring PTP Telecom Profile Clock

This procedure describes the steps involved to configure PTP clock and its settings to be consistent with ITU-T Telecom Profiles for Frequency.

Procedure

Step 1 **ptp**

Example:

```
RP/0/RP0/CPU0:router(config)# ptp
```

Enters the PTP configuration mode.

Step 2 **clock**

Example:

```
RP/0/RP0/CPU0:router(config-ptp)# clock
```

Enters the PTP-clock configuration mode.

Step 3 **domain** *domain-number*

Example:

```
RP/0/RP0/CPU0:router(config-ptp)# domain 24
```

Configures the domain number for a PTP profile. The allowed domain number range for G.8275.1 profile is between 24 and 43.

Step 4 **exit**

Example:

```
RP/0/RP0/CPU0:router(config-ptp-clock)# exit
```

Exits the PTP-clock configuration mode.

Step 5 **clock profile g.8275.1 clock-type** *clock-type*

Example:

```
RP/0/RP0/CPU0:router(config-ptp-clock)# clock profile g.8275.1 clock-type T-GM
```

Configures the desired telecom profile and the clock type for the profile.

Prerequisites for Configuring Ethernet OAM

Before configuring Ethernet OAM, confirm that at least one of the Ethernet line cards is installed on the router.

- NCS4K-2H10T-OP-KS
- NCS4K-4H-OPW-QC2

Restrictions for Configuring Ethernet OAM

Table 38: Feature History

Feature Name	Release Information	Feature Description
Hardware Timestamping Support on Multi-chassis	Cisco IOS XR Release 6.5.32	Hardware timestamping is supported for both one-way and two-way delay measurements in multi-chassis.

The following functional areas of Ethernet OAM are not supported:

- CFM is not supported on dot1q second-dot1q any and dot1ad dot1q any.
- CFM is not supported for offload session which does not have short MA name.
- Sender-ID TLV is not supported for offloaded session.
- From R6.5.28, CFM supports Y.1731 Performance Measurement i.e Delay Measurement(DMM), Loss Measurement(LMM) and Synthetic Measurement(SLM).
- From 6.5.28, software timestamping is supported for both one-way and two-way delay measurements.
- From 6.5.31, hardware timestamping is supported for both one-way and two-way delay measurements on a single chassis.
- From 6.5.32, hardware timestamping is supported for both one-way and two-way delay measurements on multi-chassis.
- CFM down-meps are not supported on L3 interface.
- CFM does not support rewrite scenarios for vlan defaults and for translate 2 to 1.
- CFM does not support MIP CCM Learning.
- CFM on Cisco IOS XR Software does not support a tag stack of more than two tags.
- If a subinterface is configured that matches untagged Ethernet frames (for example, by configuring the **encapsulation default** command), then you can not create a down MEP on the underlying physical or bundle interface.

- Both up MEPs and down MEPs are not supported on Layer 3 interfaces.
- While performing RPVM Switch Over or RP OIR or ISSU, the packet transmission stops for a duration of 3 to 20 seconds and causes EOAM session to flap (session goes down and recovers back).

Information About Configuring Ethernet OAM

To configure Ethernet OAM, you should understand the following concepts:

Ethernet Link OAM

Ethernet as a Metro Area Network (MAN) or a Wide Area Network (WAN) technology benefits greatly from the implementation of Operations, Administration and Maintenance (OAM) features. Ethernet link OAM features allow Service Providers to monitor the quality of the connections on a MAN or WAN. Service providers can monitor specific events, . Ethernet link OAM operates on a single, physical link and it can be configured to monitor either side or both sides of that link.

Ethernet link OAM can be configured in the following ways:

- A Link OAM profile can be configured, and this profile can be used to set the parameters for multiple interfaces.
- Link OAM can be configured directly on an interface.

  When an interface is also using a link OAM profile, specific parameters that are set in the profile can be overridden by configuring a different value directly on the interface.

An EOAM profile simplifies the process of configuring EOAM features on multiple interfaces. An Ethernet OAM profile, and all of its features, can be referenced by other interfaces, allowing other interfaces to inherit the features of that Ethernet OAM profile.

Individual Ethernet link OAM features can be configured on individual interfaces without being part of a profile. In these cases, the individually configured features always override the features in the profile.

The preferred method of configuring custom EOAM settings is to create an EOAM profile in Ethernet configuration mode and then attach it to an individual interface or to multiple interfaces.

These standard Ethernet Link OAM features are supported on the router:

Neighbor Discovery

Neighbor discovery enables each end of a link to learn the OAM capabilities of the other end and establish an OAM peer relationship. Each end also can require that the peer have certain capabilities before it will establish a session. You can configure certain actions to be taken if there is a capabilities conflict or if a discovery process times out, using the **action capabilities-conflict** or **action discovery-timeout** commands.

Ethernet CFM

Ethernet Connectivity Fault Management (CFM) is a service-level OAM protocol that provides tools for monitoring and troubleshooting end-to-end Ethernet services per VLAN. This includes proactive connectivity monitoring, fault verification, and fault isolation. CFM uses standard Ethernet frames and can be run on any physical media that is capable of transporting Ethernet service frames. Unlike most other Ethernet protocols which are restricted to a single physical link, CFM frames can transmit across the entire end-to-end Ethernet network.

CFM is defined in two standards:

- IEEE 802.1ag—Defines the core features of the CFM protocol.
- ITU-T Y.1731—Redefines, but maintains compatibility with the features of IEEE 802.1ag, and defines some additional features.

Ethernet CFM supports these functions of ITU-T Y.1731:

- ETH-CC, ETH-RDI, ETH-LB, ETH-LT—These are equivalent to the corresponding features defined in IEEE 802.1ag.

Note The Linktrace responder procedures defined in IEEE 802.1ag are used rather than the procedures defined in Y.1731; however, these are interoperable.

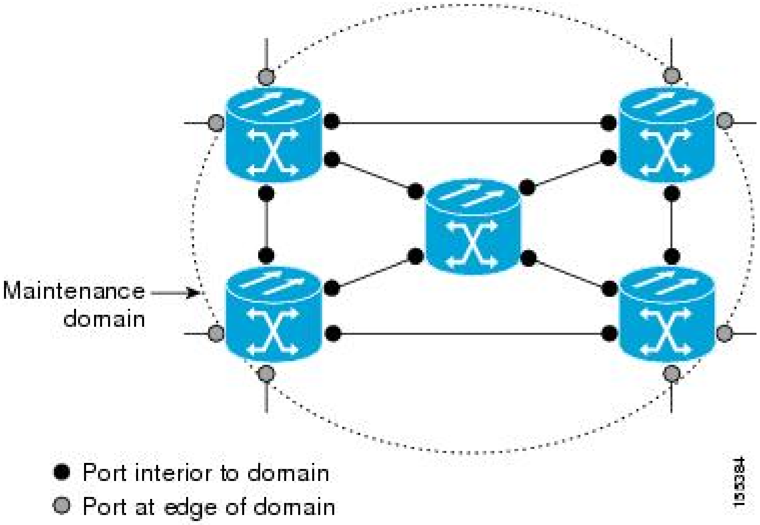
- ETH-AIS—The reception of ETH-LCK messages is also supported.

To understand how the CFM maintenance model works, you need to understand these concepts and features:

Maintenance Domains

A *maintenance domain* describes a management space for the purpose of managing and administering a network. A domain is owned and operated by a single entity and defined by the set of interfaces internal to it and at its boundary, as shown in this figure.

Figure 17: CFM Maintenance Domain



A maintenance domain is defined by the bridge ports that are provisioned within it. Domains are assigned maintenance levels, in the range of 0 to 7, by the administrator. The level of the domain is useful in defining the hierarchical relationships of multiple domains.

CFM maintenance domains allow different organizations to use CFM in the same network, but independently. For example, consider a service provider who offers a service to a customer, and to provide that service, they use two other operators in segments of the network. In this environment, CFM can be used in the following ways:

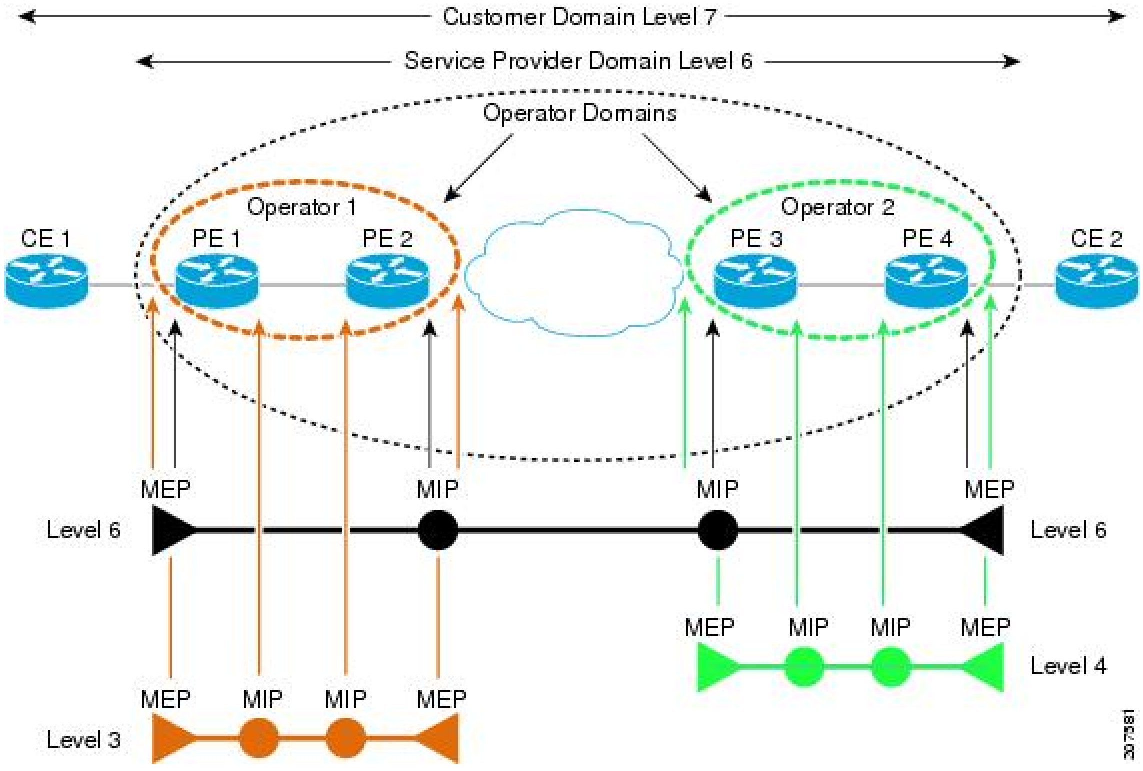
- The customer can use CFM between their CE devices, to verify and manage connectivity across the whole network.
- The service provider can use CFM between their PE devices, to verify and manage the services they are providing.
- Each operator can use CFM within their operator network, to verify and manage connectivity within their network.

Each organization uses a different CFM maintenance domain.

This figure shows an example of the different levels of maintenance domains in a network.

Note In CFM diagrams, the conventions are that triangles represent MEPs, pointing in the direction that the MEP sends CFM frames, and circles represent MIPs. For more information about MEPs and MIPs, see the Maintenance Points.

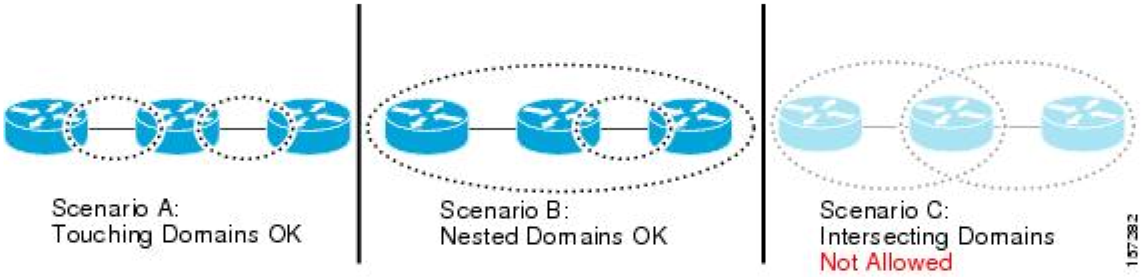
Figure 18: Different CFM Maintenance Domains Across a Network



To ensure that the CFM frames for each domain do not interfere with each other, each domain is assigned a maintenance level, between 0 and 7. Where domains are nested, as in this example, the encompassing domain must have a higher level than the domain it encloses. In this case, the domain levels must be negotiated between the organizations involved. The maintenance level is carried in all CFM frames that relate to that domain.

CFM maintenance domains may touch or nest, but cannot intersect. This figure illustrates the supported structure for touching and nested domains, and the unsupported intersection of domains.

Figure 19: Data Supported CFM Maintenance Domain Structure



Services

A CFM service allows an organization to partition its CFM maintenance domain, according to the connectivity within the network. For example, if the network is divided into a number of virtual LANs (VLANs), a CFM service is created for each of these. CFM can then operate independently in each service. It is important that the CFM services match the network topology, so that CFM frames relating to one service cannot be received in a different service. For example, a service provider may use a separate CFM service for each of their customers, to verify and manage connectivity between that customer's end points.

A CFM service is always associated with the maintenance domain that it operates within, and therefore with that domain's maintenance level. All CFM frames relating to the service carry the maintenance level of the corresponding domain.

Note CFM Services are referred to as *Maintenance Associations* in IEEE 802.1ag and as *Maintenance Entity Groups* in ITU-T Y.1731.

Maintenance Points

A CFM *Maintenance Point* (MP) is an instance of a particular CFM service on a specific interface. CFM only operates on an interface if there is a CFM maintenance point on the interface; otherwise, CFM frames are forwarded transparently through the interface.

A maintenance point is always associated with a particular CFM service, and therefore with a particular maintenance domain at a particular level. Maintenance points generally only process CFM frames at the same level as their associated maintenance domain. Frames at a higher maintenance level are always forwarded transparently, while frames at a lower maintenance level are normally dropped. This helps enforce the maintenance domain hierarchy described in the Maintenance Domains, and ensures that CFM frames for a particular domain cannot leak out beyond the boundary of the domain.

There are two types of MP:

- Maintenance End Points (MEPs)—Created at the edge of the domain. Maintenance end points (MEPs) are members of a particular service within a domain and are responsible for sourcing and sinking CFM frames. They periodically transmit continuity check messages and receive similar messages from other

MEPs within their domain. They also transmit traceroute and loopback messages at the request of the administrator. MEPs are responsible for confining CFM messages within the domain.

- Maintenance Intermediate Points (MIPs)—Created in the middle of the domain. Unlike MEPS, MIPs do allow CFM frames at their own level to be forwarded.

MIP Creation

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. The algorithm, in brief, operates as follows for each interface:

- 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 (**mip auto-create** command) 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 selected by the algorithm first.

MEP and CFM Processing Overview

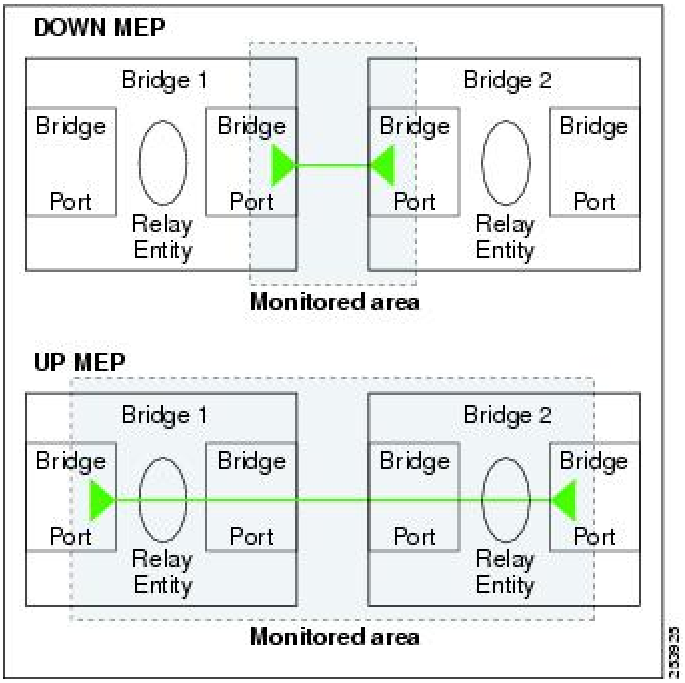
The boundary of a domain is an interface, rather than a bridge or host. Therefore, MEPs can be sub-divided into two categories:

- Down MEPs—Send CFM frames from the interface where they are configured, and process CFM frames received on that interface. Down MEPs transmit AIS messages upward (toward the cross-connect).
- Up MEPs—Send frames into the bridge relay function, as if they had been received on the interface where the MEP is configured. They process CFM frames that have been received on other interfaces, and have been switched through the bridge relay function as if they are going to be sent out of the interface where the MEP is configured. Up MEPs transmit AIS messages downward (toward the wire). However, AIS packets are only sent when there is a MIP configured on the same interface as the MEP and at the level of the MIP.

Note The terms *Down MEP* and *Up MEP* are defined in the IEEE 802.1ag and ITU-T Y.1731 standards, and refer to the direction that CFM frames are sent from the MEP. The terms should not be confused with the operational status of the MEP.

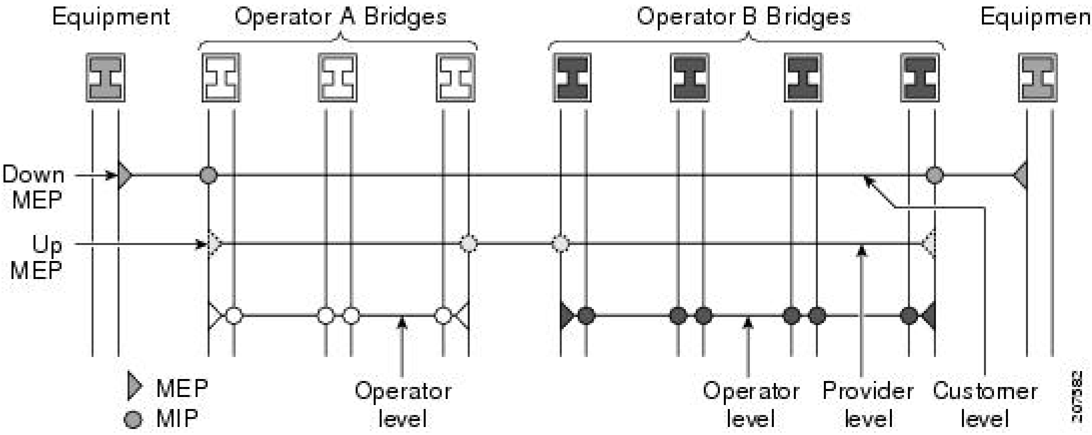
This figure illustrates the monitored areas for Down and Up MEPs.

Figure 20: Monitored Areas for Down and Up MEPs



This figure shows maintenance points at different levels. Because domains are allowed to nest but not intersect, a MEP at a low level always corresponds with a MEP or MIP at a higher level. In addition, only a single MIP is allowed on any interface—this is generally created in the lowest domain that exists at the interface and that does not have a MEP.

Figure 21: Data CFM Maintenance Points at Different Levels



MIPs and Up MEPs can only exist on switched (Layer 2) interfaces, because they send and receive frames from the bridge relay function. Down MEPs can be created on switched (Layer 2) or routed (Layer 3) interfaces.

MEPs continue to operate normally if the interface they are created on is blocked by the Spanning Tree Protocol (STP); that is, CFM frames at the level of the MEP continue to be sent and received, according to the direction of the MEP. MEPs never allow CFM frames at the level of the MEP to be forwarded, so the STP block is maintained.

MIPs also continue to receive CFM frames at their level if the interface is STP blocked, and can respond to any received frames. However, MIPs do not allow CFM frames at the level of the MIP to be forwarded if the interface is blocked.

Note A separate set of CFM maintenance levels is created every time a VLAN tag is pushed onto the frame. Therefore, if CFM frames are received on an interface which pushes an additional tag, so as to "tunnel" the frames over part of the network, the CFM frames will not be processed by any MPs within the tunnel, even if they are at the same level. For example, if a CFM MP is created on an interface with an encapsulation that matches a single VLAN tag, any CFM frames that are received at the interface that have two VLAN tags will be forwarded transparently, regardless of the CFM level.

CFM Protocol Messages

The CFM protocol consists of a number of different message types, with different purposes. All CFM messages use the CFM EtherType, and carry the CFM maintenance level for the domain to which they apply.

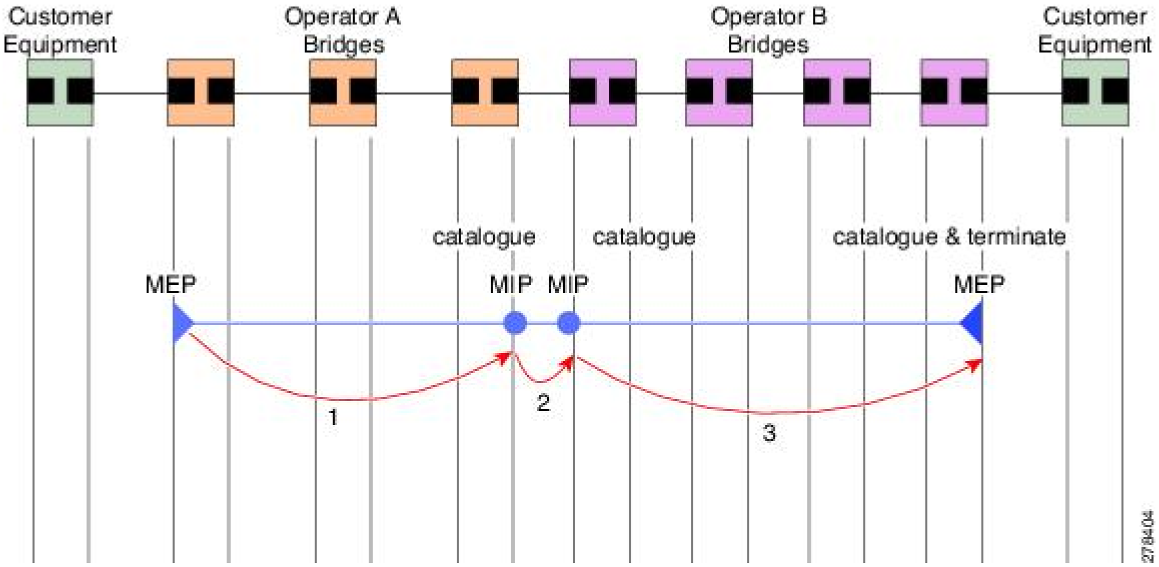
This section describes the following CFM messages:

Continuity Check (IEEE 802.1ag and ITU-T Y.1731)

Continuity Check Messages (CCMs) are "heartbeat" messages exchanged periodically between all the MEPs in a service. Each MEP sends out multicast CCMs, and receives CCMs from all the other MEPs in the service—these are referred to as *peer MEPs*. This allows each MEP to discover its peer MEPs, and to verify that there is connectivity between them.

MIPs also receive CCMs. MIPs use the information to build a MAC learning database that is used when responding to Linktrace.

Figure 22: Continuity Check Message Flow



All the MEPs in a service must transmit CCMs at the same interval. IEEE 802.1ag defines 7 possible intervals that can be used:

- 10ms

- 100ms
- 1s
- 10s
- 1 minute
- 10 minutes

A MEP detects a loss of connectivity with one of its peer MEPs when some number of CCMs have been missed. This occurs when sufficient time has passed during which a certain number of CCMs were expected, given the CCM interval. This number is called the *loss threshold*, and is usually set to 3.

CCM messages carry a variety of information that allows different defects to be detected in the service. This information includes:

- A configured identifier for the domain of the transmitting MEP. This is referred to as the Maintenance Domain Identifier (MDID).
- A configured identifier for the service of the transmitting MEP. This is referred to as the Short MA Name (SMAN). Together, the MDID and the SMAN make up the Maintenance Association Identifier (MAID). The MAID must be configured identically on every MEP in the service.
- A configured numeric identifier for the MEP (the MEP ID). Each MEP in the service must be configured with a different MEP ID.
- A sequence number.
- A Remote Defect Indication (RDI). Each MEP includes this in the CCMs it is sending, if it has detected a defect relating to the CCMs it is receiving. This notifies all the MEPs in the service that a defect has been detected somewhere in the service.
- The interval at which CCMs are being transmitted.
- The status of the interface where the MEP is operating—for example, whether the interface is up, down, STP blocked, and so on.

Note The status of the interface (up/down) should not be confused with the direction of any MEPs on the interface (Up MEPs/Down MEPs).

These defects can be detected from received CCMs:

- Interval mismatch—The CCM interval in the received CCM does not match the interval that the MEP is sending CCMs.
- Level mismatch—A MEP has received a CCM carrying a lower maintenance level than the MEPs own level.
- Loop—A CCM is received with the source MAC address equal to the MAC address of the interface where the MEP is operating.
- Configuration error—A CCM is received with the same MEP ID as the MEP ID configured for the receiving MEP.

- Cross-connect—A CCM is received with an MAID that does not match the locally configured MAID. This generally indicates a VLAN misconfiguration within the network, such that CCMs from one service are leaking into a different service.
- Peer interface down—A CCM is received that indicates the interface on the peer is down.
- Remote defect indication—A CCM is received carrying a remote defect indication.

Note This defect does not cause the MEP to include a remote defect indication in the CCMs that it is sending.

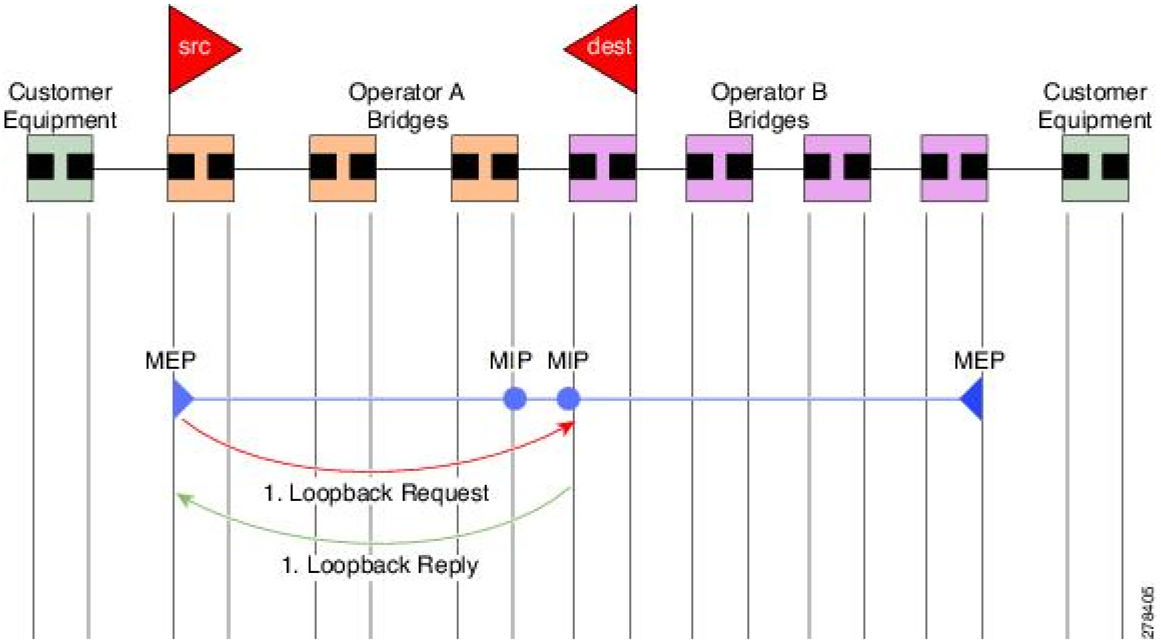
Out-of-sequence CCMs can also be detected by monitoring the sequence number in the received CCMs from each peer MEP. However, this is not considered a CCM defect.

Loopback (IEEE 802.1ag and ITU-T Y.1731)

Loopback Messages (LBM) and Loopback Replies (LBR) are used to verify connectivity between a local MEP and a particular remote MP. At the request of the administrator, a local MEP sends unicast LBMs to the remote MP. On receiving each LBM, the target maintenance point sends an LBR back to the originating MEP. Loopback indicates whether the destination is reachable or not—it does not allow hop-by-hop discovery of the path. It is similar in concept to an ICMP Echo (ping). Since loopback messages are destined for unicast addresses, they are forwarded like normal data traffic, while observing the maintenance levels. At each device that the loopback reaches, if the outgoing interface is known (in the bridge's forwarding database), then the frame is sent out on that interface. If the outgoing interface is not known, then the message is flooded on all interfaces.

This figure shows an example of CFM loopback message flow between a MEP and MIP.

Figure 23: Loopback Messages



Loopback messages can be padded with user-specified data. This allows data corruption to be detected in the network. They also carry a sequence number which allows for out-of-order frames to be detected.

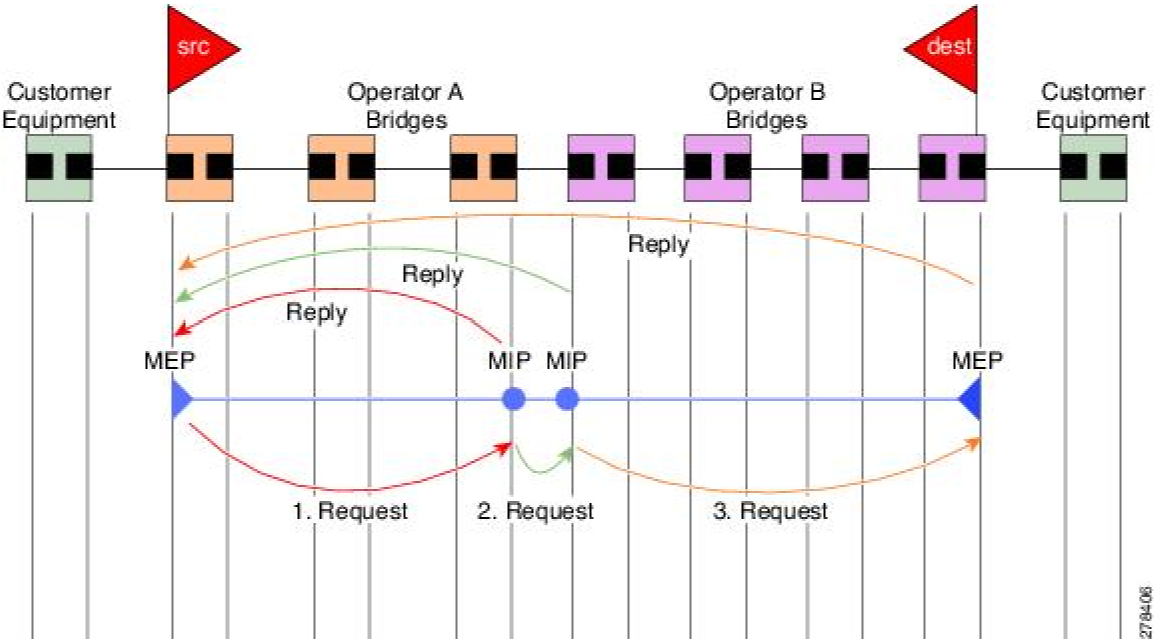
Note The Ethernet CFM loopback function should not be confused with the remote loopback functionality in Ethernet Link OAM. CFM loopback is used to test connectivity with a remote MP, and only the CFM LBM packets are reflected back, but Ethernet Link OAM remote loopback is used to test a link by taking it out of normal service and putting it into a mode where it reflects back all packets.

Linktrace (IEEE 802.1ag and ITU-T Y.1731)

Linktrace Messages (LTM) and Linktrace Replies (LTR) are used to track the path (hop-by-hop) to a unicast destination MAC address. At the request of the operator, a local MEP sends an LTM. Each hop where there is a maintenance point sends an LTR back to the originating MEP. This allows the administrator to discover connectivity data about the path. It is similar in concept to IP traceroute, although the mechanism is different. In IP traceroute, successive probes are sent, whereas CFM Linktrace uses a single LTM which is forwarded by each MP in the path. LTMs are multicast, and carry the unicast target MAC address as data within the frame. They are intercepted at each hop where there is a maintenance point, and either retransmitted or dropped to discover the unicast path to the target MAC address.

This figure shows an example of CFM linktrace message flow between MEPs and MIPs.

Figure 24: Linktrace Message Flow



The linktrace mechanism is designed to provide useful information even after a network failure. This allows it to be used to locate failures, for example after a loss of continuity is detected. To achieve this, each MP maintains a CCM Learning Database. This maps the source MAC address for each received CCM to the interface through which the CCM was received. It is similar to a typical bridge MAC learning database, except that it is based only on CCMs and it times out much more slowly—on the order of days rather than minutes.

Note In IEEE 802.1ag, the CCM Learning Database is referred to as the MIP CCM Database. However, it applies to both MIPs and MEPs.

In IEEE 802.1ag, when an MP receives an LTM message, it determines whether to send a reply using the following steps:

1. The target MAC address in the LTM is looked up in the bridge MAC learning table. If the MAC address is known, and therefore the egress interface is known, then an LTR is sent.
2. If the MAC address is not found in the bridge MAC learning table, then it is looked up in the CCM learning database. If it is found, then an LTR is sent.
3. If the MAC address is not found, then no LTR is sent (and the LTM is not forwarded).

If the target MAC has never been seen previously in the network, the linktrace operation will not produce any results.

Note IEEE 802.1ag and ITU-T Y.1731 define slightly different linktrace mechanisms. In particular, the use of the CCM learning database and the algorithm described above for responding to LTM messages are specific to IEEE 802.1ag. IEEE 802.1ag also specifies additional information that can be included in LTRs. Regardless of the differences, the two mechanisms are interoperable.

Exploratory Linktrace (Cisco)

Exploratory Linktrace is a Cisco extension to the standard linktrace mechanism described above. It has two primary purposes:

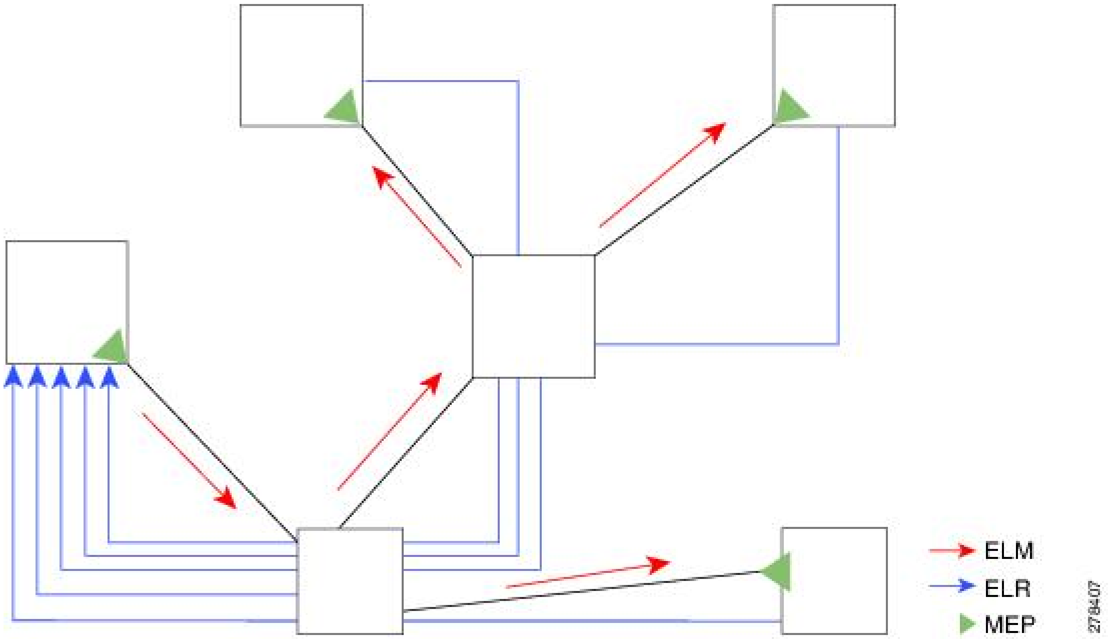
- Provide a mechanism to locate faults in cases where standard linktrace does not work, such as when a MAC address has never been seen previously in the network. For example, if a new MEP has been provisioned but is not working, standard linktrace does not help isolate a problem because no frames will ever have been received from the new MEP. Exploratory Linktrace overcomes this problem.
- Provide a mechanism to map the complete active network topology from a single node. This can only be done currently by examining the topology (for example, the STP blocking state) on each node in the network individually, and manually combining this information to create the overall active topology map. Exploratory linktrace allows this to be done automatically from a single node.

Exploratory Linktrace is implemented using the Vendor Specific Message (VSM) and Vendor Specific Reply (VSR) frames defined in ITU-T Y.1731. These allow vendor-specific extensions to be implemented without degrading interoperability. Exploratory Linktrace can safely be deployed in a network that includes other CFM implementations because those implementations will simply ignore the Exploratory Linktrace messages.

Exploratory Linktrace is initiated at the request of the administrator, and results in the local MEP sending a multicast Exploratory Linktrace message. Each MP in the network that receives the message sends an Exploratory Linktrace reply. MIPs that receive the message also forward it on. The initiating MEP uses all the replies to create a tree of the overall network topology.

This figure show an example of the Exploratory Linktrace message flow between MEPs.

Figure 25: Exploratory Linktrace Messages and Replies



To avoid overloading the originating MEP with replies in a large network, responding MPs delay sending their replies for a random amount of time, and that time increases as the size of the network increases.

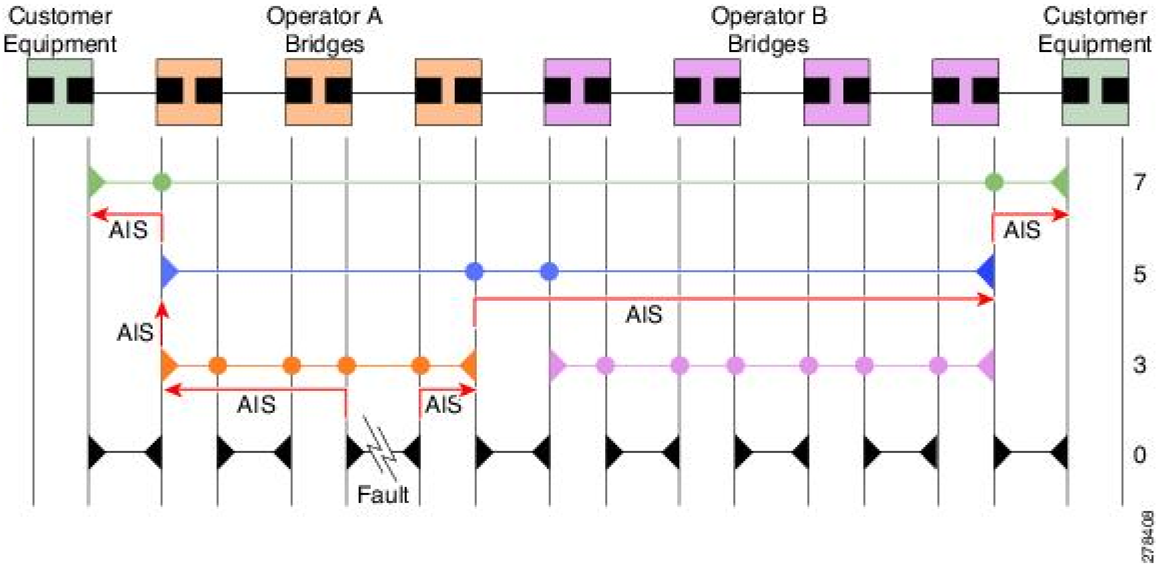
In a large network, there will be a corresponding large number of replies and the resulting topology map will be equally large. If only a part of the network is of interest, for example, because a problem has already been narrowed down to a small area, then the Exploratory Linktrace can be "directed" to start at a particular MP. Replies will thus only be received from MPs beyond that point in the network. The replies are still sent back to the originating MEP.

Alarm Indication Signal (ITU-T Y.1731)

Alarm Indication Signal (AIS) messages are used to rapidly notify MEPs when a fault is detected in the middle of a domain, in an event driven way. MEPs thereby learn of the fault much sooner than if they relied on detecting a loss of continuity, for example, failure to receive some number of consecutive CCMs.

Unlike all other CFM messages, AIS messages are injected into the middle of a domain, and sent outward toward the MEPs at the edge of the domain. Typically, AIS messages are injected by a MEP in a lower level domain. To put it another way, when a MEP sends AIS messages, they are sent in the opposite direction to other CFM messages sent by the MEP, and at a level above the MEP's own level. The AIS messages are received by the MEPs in the higher level domain, not by the peer MEPs in the same domain as the MEP sending the AIS. When a MEP receives an AIS message, it may itself send another AIS message at an even higher level.

Figure 26: AIS Message Flow



AIS is only applicable in point-to-point networks. In multipoint networks with redundant paths, a failure at a low level does not necessarily result in a failure at a higher level, as the network may reconverge so as to route around the failed link.

AIS messages are typically sent by a MEP. However, AIS messages can also be sent when there is no MEP present, if a fault is detected in the underlying transport, such as if an interface goes down. In ITU-T Y.1731 these are referred to as server MEPs.

AIS messages are sent in response to a number of failure conditions:

- Detection of CCM defects, as described Continuity Check (IEEE 802.1ag and ITU-T Y.1731), on page 486.
- Loss of continuity.
- Receipt of AIS messages.
- Failure in the underlying transport, such as when an interface is down.

Received AIS messages can be used to detect and act on failures more quickly than waiting for a loss of continuity. They can also be used to suppress any failure action, on the basis that the failure has already been detected at a lower level and will be handled there. This is described in ITU-T Y.1731; however, the former is often more useful.

MEP Cross-Check

MEP cross-check supports configuration of a set of expected peer MEPs so that errors can be detected when any of the known MEPs are missing, or if any additional peer MEPs are detected that are not in the expected group.

The set of expected MEP IDs in the service is user-defined. Optionally, the corresponding MAC addresses can also be specified. CFM monitors the set of peer MEPs from which CCMs are being received. If no CCMs are ever received from one of the specified expected peer MEPs, or if a loss of continuity is detected, then a cross-check “missing” defect is detected. Similarly, if CCMs are received from a matching MEP ID but with the wrong source MAC address, a cross-check “missing” defect is detected. If CCMs are subsequently received that match the expected MEP ID, and if specified, the expected MAC address, then the defect is cleared.

Note In NCS4K, CFM cross-check is mandatory for CFM offloaded session. Cross-check feature can be configured with or without mac address option. Cross-check is not mandatory for non-offloaded session.

If cross-check is configured and CCMs are received from a peer MEP with a MEP ID that is not expected, this is detected as a cross-check “unexpected” condition.

Configurable Logging

CFM supports logging of various conditions to syslog. Logging can be enabled independently for each service, and when the following conditions occur:

- New peer MEPs are detected, or loss of continuity with a peer MEP occurs.
- Changes to the CCM defect conditions are detected.
- Cross-check “missing” or “unexpected” conditions are detected.
- AIS condition detected (AIS messages received) or cleared (AIS messages no longer received).
- EFD used to shut down an interface, or bring it back up.

EFD

Ethernet Fault Detection (EFD) is a mechanism that allows Ethernet OAM protocols, such as CFM, to control the “line protocol” state of an interface.

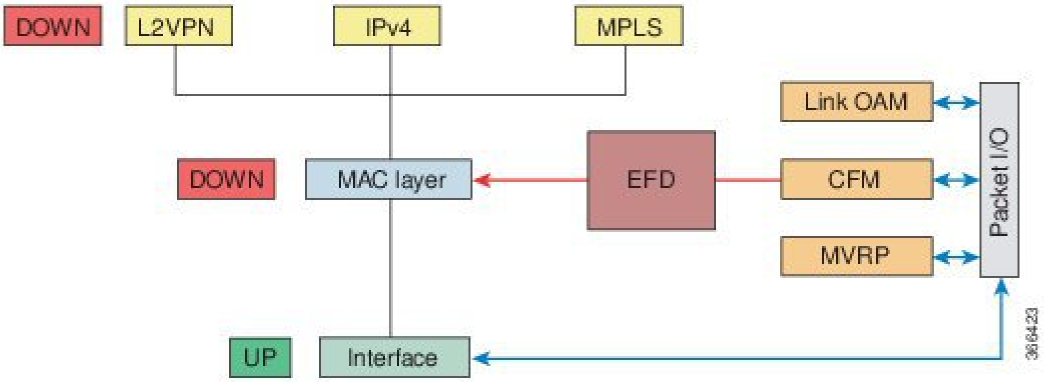
Unlike many other interface types, Ethernet interfaces do not have a line protocol, whose state is independent from that of the interface. For Ethernet interfaces, this role is handled by the physical-layer Ethernet protocol itself, and therefore if the interface is physically up, then it is available and traffic can flow.

EFD changes this to allow CFM to act as the line protocol for Ethernet interfaces. This allows CFM to control the interface state so that if a CFM defect (such as AIS or loss of continuity) is detected with an expected peer MEP, the interface can be shut down. This not only stops any traffic flowing, but also triggers actions in any higher-level protocols to route around the problem. For example, in the case of Layer 2 interfaces, the MAC table would be cleared and MSTP would reconverge. For Layer 3 interfaces, the ARP cache would be cleared and potentially the IGP would reconverge.

Note EFD can only be used for down MEPs. When EFD is used to shut down the interface, the CFM frames continue to flow. This allows CFM to detect when the problem has been resolved, and thus bring the interface backup automatically.

This figure shows CFM detection of an error on one of its sessions EFD signaling an error to the corresponding MAC layer for the interface. This triggers the MAC to go to a down state, which further triggers all higher level protocols (Layer 2 pseudowires, IP protocols, and so on) to go down and also trigger a reconvergence where possible. As soon as CFM detects there is no longer any error, it can signal to EFD and all protocols will once again go active.

Figure 27: CFM Error Detection and EFD Trigger



Flexible VLAN Tagging for CFM

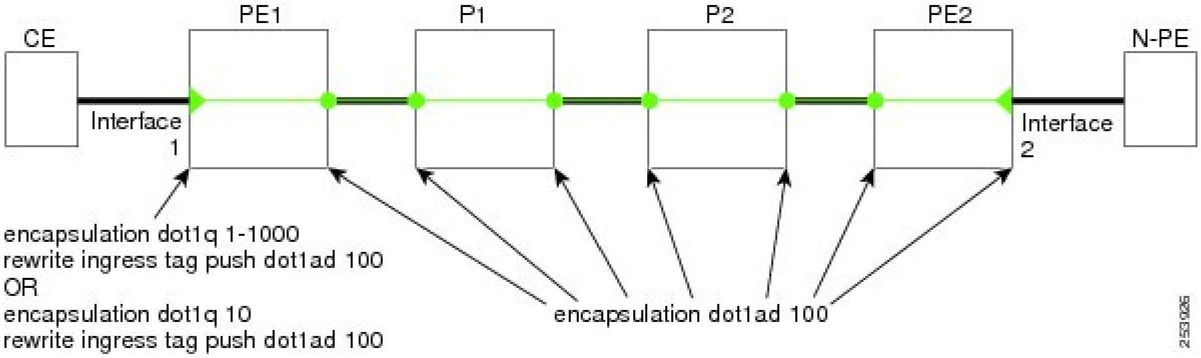
The Flexible VLAN Tagging for CFM feature ensures that CFM packets are sent with the right VLAN tags so that they are appropriately handled as a CFM packet by the remote device. When packets are received by an edge router, they are treated as either CFM packets or data packets, depending on the number of tags in the header. The system differentiates between CFM packets and data packets based on the number of tags in the packet, and forwards the packets to the appropriate paths based on the number of tags in the packet.

CFM frames are normally sent with the same VLAN tags as the corresponding customer data traffic on the interface, as defined by the configured encapsulation and tag rewrite operations. Likewise, received frames are treated as CFM frames if they have the correct number of tags as defined by the configured encapsulation and tag rewrite configuration, and are treated as data frames (that is, they are forwarded transparently) if they have more than this number of tags.

In most cases, this behavior is as desired, since the CFM frames are then treated in exactly the same way as the data traffic flowing through the same service. However, in a scenario where multiple customer VLANs are multiplexed over a single multipoint provider service (for example, N:1 bundling), a different behavior might be desirable.

This figure shows an example of a network with multiple VLANS using CFM.

Figure 28: Service Provider Network With Multiple VLANs and CFM


CE
PE1
P1
P2
PE2
N-PE
Interface 1
Interface 2
encapsulation dot1q 1-1000
rewrite ingress tag push dot1ad 100
OR
encapsulation dot1q 10
rewrite ingress tag push dot1ad 100
encapsulation dot1ad 100
253926

This figure shows a provider's access network, where the S-VLAN tag is used as the service delimiter. PE1 faces the customer, and PE2 is at the edge of the access network facing the core. N:1 bundling is used, so the interface encapsulation matches a range of C-VLAN tags. This could potentially be the full range, resulting in all:1 bundling. There is also a use case where only a single C-VLAN is matched, but the S-VLAN is nevertheless used as the service delimiter—this is more in keeping with the IEEE model, but limits the provider to 4094 services.

CFM is used in this network with a MEP at each end of the access network, and MIPs on the boxes within the network (if it is native Ethernet). In the normal case, CFM frames are sent by the up MEP on PE1 with two VLAN tags, matching the customer data traffic. This means that at the core interfaces and at the MEP on PE2, the CFM frames are forwarded as if they were customer data traffic, since these interfaces match only on the S-VLAN tag. So, the CFM frames sent by the MEP on PE1 are not seen by any of the other MPs.

Flexible VLAN tagging changes the encapsulation for CFM frames that are sent and received at Up MEPs. Flexible VLAN tagging allows the frames to be sent from the MEP on PE1 with just the S-VLAN tag that represents the provider service. If this is done, the core interfaces will treat the frames as CFM frames and they will be seen by the MIPs and by the MEP on PE2. Likewise, the MEP on PE1 should handle received frames with only one tag, as this is what it will receive from the MEP on PE2.

To ensure that CFM packets from Up MEPs are routed to the appropriate paths successfully, tags may be set to a specific number in a domain service, using the **tags** command. Currently, tags can only be set to one (1).

CFM Scale Details

The following table has CFM scale details:

Packet Type	Scale
CCM	2000 per LC, 8000 per system
AIS	2000 per LC, 8000 per system
SLM	2000 per LC, 8000 per system
Two-way DM	2000 per LC, 8000 per system

The scale numbers indicated in the above table are applicable for single chassis and multi chassis systems.

Ethernet SLA

Customers require their service providers to conform to a Service Level Agreement (SLA). Consequently, service providers must be able to monitor the performance characteristics of their networks. Similarly, customers also want to monitor the performance characteristics of their networks. Cisco provides Y.1731 performance monitoring using the Cisco Ethernet SLA feature.

The Cisco Ethernet SLA feature provides the architecture to monitor a network at Layer 2. This architecture provides functions such as collecting, storing, displaying, and analyzing SLA statistics. These SLA statistics can be stored and displayed in various ways, so that statistical analysis can be performed.

Ethernet SLA provides the framework for performing the following major functions of performance monitoring:

- Sending probes consisting of one or more packets to measure performance.

  Ethernet SLA provides a flexible mechanism for sending SLA probes to measure performance. Probes can consist of either CFM loopback, CFM loss measurement packets, or CFM delay measurement packets.

Options are available to modify how often the packets are sent, and to specify the attributes of the probe packets such as the size and priority.

- Scheduling of operations consisting of periodic probes.

  A flexible mechanism is provided by Ethernet SLA to specify how often each probe should be executed, how long it should last, and when the first probe should start. Probes can be scheduled to run back-to-back to provide continuous measurements, or at a defined interval ranging from once a minute to once a week.

- Collecting and storing results.

  Ethernet SLA provides flexibility to specify which performance parameters should be collected and stored for each measurement probe. Performance parameters include frame delay and jitter (inter-frame delay variation). For each performance parameter, either each individual result can be stored, or the results can be aggregated by storing a counter of the number of results that fall within a particular range. A configurable amount of historical data can also be stored as well as the latest results.

- Analyzing and displaying results.

  Ethernet SLA performs some basic statistical analysis on the collected results, such as calculating the minimum, maximum, mean and standard deviation. It also records whether any of the probe packets were lost or misordered, or if there is any reason why the results may not be a true reflection of the performance (for example if a big jump in the local time-of-day clock was detected during the time when the measurements were being made).

Ethernet SLA Measurement Packet

An Ethernet SLA *measurement packet* is a single protocol message and corresponding reply that is sent on the network for the purpose of making SLA measurements. These types of measurement packet are supported:

- CFM Delay Measurement (Y.1731 DMM/DMR packets)—CFM delay measurement packets contain timestamps within the packet data that can be used for accurate measurement of frame delay and jitter. These packets can be used to measure round-trip statistics; however, the size of the DMM/DMR packets cannot be modified.

Note Delay measurement can be performed only after the PTP is configured and the clocks are in sync. See Understanding PTP, on page 475.

- CFM loopback (LBM/LBR)—CFM loopback packets are less accurate, but can be used if the peer device does not support DMM/DMR packets. Only round-trip statistics can be measured because these packets do not contain timestamps. However, loopback packets can be padded, so measurements can be made using frames of a specific size.

- CFM Synthetic Loss Measurement (Y.1731 SLM/SLR packets)—SLM packets contain two sequence numbers; one written by the initiator into the SLM and copied by the responder into the SLR, and the other allocated by the responder and written into the SLR. These are refered to as the source-to-destination (sd) sequence number and the destination-to-source (ds) sequence number respectively.

Ethernet SLA Sample

A *sample* is a single result—a number—that relates to a given statistic. For some statistics such as round-trip delay, a sample can be measured using a single measurement packet. For other statistics such as jitter, obtaining a sample requires two measurement packets.

Ethernet SLA Probe

A *probe* is a sequence of measurement packets used to gather SLA samples for a specific set of statistics. The measurement packets in a probe are of a specific type (for example, CFM delay measurement or CFM loopback) and have specific attributes, such as the frame size and priority.

Ethernet SLA Burst

Within a probe, measurement packets can either be sent individually, or in bursts. A *burst* contains two or more packets sent within a short interval. Each burst can last up to one minute, and bursts can follow each other immediately to provide continuous measurement within the probe.

For statistics that require two measurement packets for each sample, samples are only calculated based on measurement packets in the same burst. For all statistics, it is more efficient to use bursts than to send individual packets.

Ethernet SLA Schedule

An Ethernet SLA *schedule* describes how often probes are sent, how long each probe lasts, and at what time the first probe starts.

Ethernet SLA Bucket

For a particular statistic, a *bucket* is a collection of results that were gathered during a particular period of time. All of the samples for measurements that were initiated during the period of time represented by a bucket are stored in that bucket. Buckets allow results from different periods of time to be compared (for example, peak traffic to off-peak traffic).

By default, a separate bucket is created for each probe; that is, the bucket represents the period of time starting at the same time as the probe started, and continuing for the duration of the probe. The bucket will therefore contain all the results relating to measurements made by that probe.

Ethernet SLA Operation

An *operation* is an instance of a given operation profile that is actively collecting performance data. Operation instances are created by associating an operation profile with a given source (an interface and MEP) and with a given destination (a MEP ID or MAC address). Operation instances exist for as long as the configuration is applied, and they run for an indefinite duration on an ongoing basis.

Ethernet SLA On-Demand Operation

An *on-demand operation* is a method of Ethernet SLA operation that can be run on an as-needed basis for a specific and finite period of time. This can be useful in situations such as when you are starting a new service or modifying the parameters for a service to verify the impact of the changes, or if you want to run a more detailed probe when a problem is detected by an ongoing scheduled operation.

On-demand operations do not use profiles and have a finite duration. The statistics that are collected are discarded after a finite time after the operation completes (two weeks), or when you manually clear them. On-demand operations do not persist across a card reload.

Configuring SLA Operation

This section describes how to configure an ongoing SLA operation on a MEP using an SLA profile.

Procedure

Step 1 **interface** *type* **R/S/I/P**

Example:

```
RP/0/RP0:router(config)# interface gigabitethernet 0/1/0/1
```

Enters the interface configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:router(config-if)# ethernet cfm
```

Enters the CFM configuration mode.

Step 3 **mep domain** *domain_name* **service** *service_name* **mep-id** *number*

Example:

```
RP/0/RP0:router(config-if-cfm)# mep domain d1 service Sv1 mep-id 2
```

Creates a MEP on an interface and enters interface CFM MEP configuration mode.

Step 4 **sla operation profile** *profile_name* **target** s{ **mep-id** *id* | **mac-address** *address*}

Example:

```
RP/0/RP0:router(config-if-cfm-mep)# sla operation profile p1 target mac-address 01:23:45:67
```

Creates an operation instance from a MEP to a specified destination.

Step 5 **commit or end**

Saves the configuration changes; when you issue the **end** command, the system prompts you to commit the changes.

Configuring SLA Probe Profile

To configure SLA probe parameters in a profile, perform these steps beginning in SLA profile configuration mode.

Procedure

Step 1 **probe**

Example:

```
RP/0/RP0:router(config-sla-profile) # probe
```

Enters the SLA profile probe configration mode.

Step 2 **send** { **burst** | **packet** } { **every** *number* { **seconds** | **minutes** | **hours** } | **once** } } **packet count** *packets* **interval** *number* { **seconds** | **milliseconds** }

Example:

```
RP/0/RP0:router(config-sla-prof-pb)# send burst every 60 seconds packet count 100 interval
 100 milliseconds
```

Sets the parameters for burst or packet.

Step 3 **packet size** *bytes* [**test-pattern** { **hex 0xHHHHHHHH** | **pseudo-random** }]

Example:

```
RP/0/RP0:router(config-sla-prof-pb)# packet size 9000
```

Configures the minimum size (in bytes) for outgoing probe packets, including padding when necessary. Use the test pattern keyword to specify a hexadecimal string to use as the padding characters, or a pseudo-random bit sequence. The default padding is 0’s. The packet size can be configured for SLM, loopback, and DMM/R probes.

Step 4 **priority**

Example:

```
RP/0/RP0:router(config-sla-prof-pb)# priority 7
```

Configures the priority of outgoing SLA probe packets.

Step 5 **synthetic loss calculation packets** *number*

Example:

```
RP/0/RP0:router(config-sla-prof-pb)# synthetic loss calculation packets 25
```

Configures the number of packets that must be used to make each frame loss ratio calculation in the case of synthetic loss measurements. This item can only be configured for packet types that support synthetic loss measurement.

Step 6 **commit or end**

Saves the configuration. When you use the **end** command, the system prompts the user to commit the changes.

Configuring SLA Operation Profile

This task has details about configuring an SLA operation profile. You can configure only up to hundred SLA operation profiles.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:router# config
```

Enters the global configuration mode.

Step 2 **ethernet sla**

Example:

```
RP/0/RP0/CPU0:router (config)# ethernet sla
```

Enters the SLA configuration mode.

Step 3 **profile** *profile-name* **type** {**cfm-delay-measurement** | **cfm-loopback** | **cfm-synthetic-loss-measurement** }

Example:

```
RP/0/RP0/CPU0:router(config-sla)# profile  profile1 type cfm-synthetic-loss-measurement
```

Creates an SLA operation profile and enters the SLA profile configuration mode.

Step 4 **commit or end**

Saves the configuration changes; when you issue the **end** command, the system prompts you to commit the changes.

Configuring SLA Statisics Profile

The Ethernet SLA feature supports measurement of two-way delay and jitter statistics.

To configure SLA statistics measurement in a profile, perform these steps beginning in SLA profile configuration mode.

Procedure

Step 1 **statistics measure** {**round-trip-delay** | **round-trip-jitter**}

Example:

```
RP/0/RP0:router(config-sla-prof)# statistics measure round-trip-delay
```

Enables the collection of SLA statistics, and enters SLA profile statistics configuration mode.

Step 2 **aggregate** {**bins** *count* **width** *width* | **none**}

Example:

```
RP/0/RP0:router(config-sla-prof-stat-cfg)# aggregate bins 100 width 10000
```

Configures the size and number of bins into which to aggregate the results of statistics collection. For delay measurements and data loss measurements, the default is that all values are aggregated into 1 bin. For synthetic loss measurements, the default is aggregation disabled.

Step 3 **buckets size** *number* {**probes**}

Example:

```
RP/0/RP0:router(config-sla-prof-stat-cfg)# buckets size 100 probes
```

Configures the size of the buckets in which statistics are collected.

Step 4 **buckets archive** *number*

Example:

```
RP/0/RP0:router(config-sla-prof-stat-cfg)# buckets archive 50
```

Configures the number of buckets to store in memory.

Step 5 **end or commit**

Saves the configuration changes; if you issue the **end** command, the system will prompt you to commit.

Requesting On-Demand Ethernet SLA for CFM Delay Measurement

This task has details about requesting an on-demand ethernet SLA operation for CFM delay measurement.

Procedure

ethernet sla on-demand operation type cfm-delay-measurement probe [**prority** *number*] [**send** { **packet** | **burst** *imterval* }] **domain** *domain name* **source interface** *type* **R/S/I/P** **target** { **mac-address** *address* | **mep-id***id* } [**statistics measure** { **round-trip-delay** | **round-trip-jitter** }] [**schedule** { **now** | **at** *time*] [**for duration** { **seconds** | **minutes** | **hours** }]

Example:

```
RP/0/RP0:router # ethernet sla on-demand operation type cfm-delay-measurement probe domain
 D1 source interface TenGigE 0/6/1/0 target mep-id 100
```

Configures an on-demand Ethernet SLA operation for CFM delay measurement.

Note This command is in EXEC mode.

Configuring On-Demand Ethernet SLA for CFM Synthetic Loss Measurement

This task has details about configuring an on-demand ethernet SLA operation for CFM synthetic loss measurement.

Procedure

ethernet sla on-demand operation type cfm-synthetic-loss-measurement probe [**prority** *number*] [**send** { **packet** | **burst** *imterval* }] **domain** *domain name* **source interface** *type* **R/S/I/P** **target** { **mac-address** *address* | **mep-id***id* } [**synthetic loss calculation packets** *number*] [**statistics measure** { **round-trip-loss-ds** | **round-trip-loss-sd** }] [**schedule** { **now** | **at** *time*] [**for duration** { **seconds** | **minutes** | **hours** }]

Example:

```
RP/0/RP0:router (config)# ethernet sla on-demand operation type cfm-synthetic-loss-measurement
 probe domain D1 source interface TenGigE 0/6/1/0 target mac-address 2.3.4
```

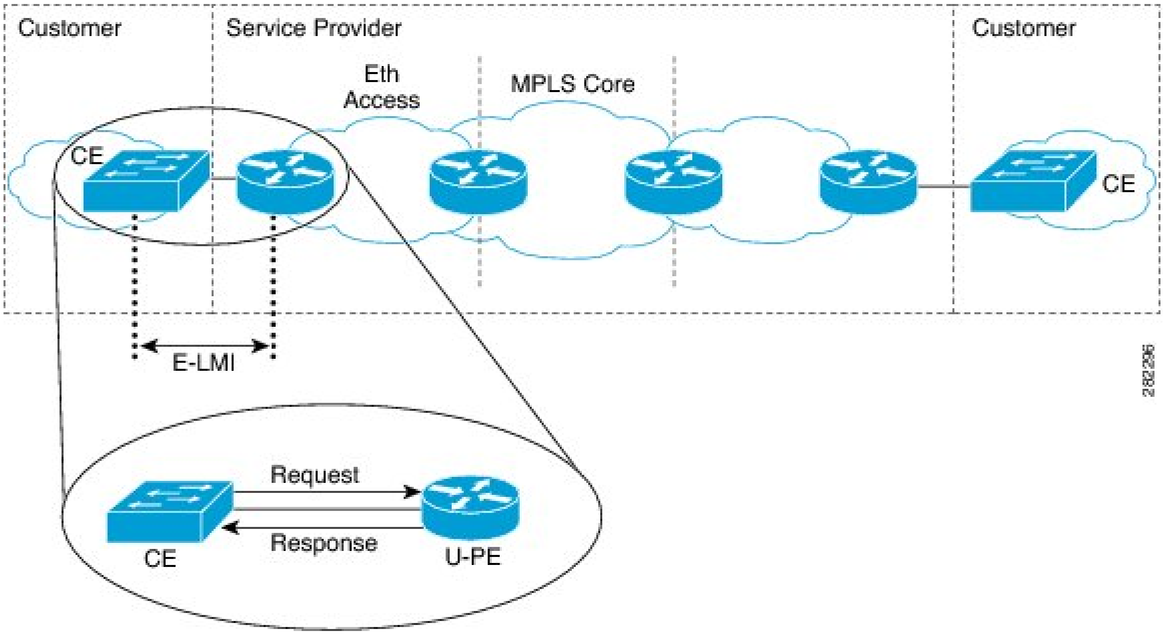
Configures an on-demand Ethernet SLA operation for CFM synthetic measurement.

Note This command is in EXEC mode.

Ethernet LMI

E-LMI runs on the link between the customer-edge (CE) device and the provider-edge (PE) device, or User Network Interface (UNI), and provides a way for the CE device to auto-configure or monitor the services offered by the PE device (see this figure).

Figure 29: E-LMI Communication on CE-to-PE Link



E-LMI is an asymmetric protocol whose basic operation involves the User-facing PE (uPE) device providing connectivity status and configuration parameters to the CE using STATUS messages in response to STATUS ENQUIRY messages sent by the CE to the uPE.

E-LMI Messaging

The E-LMI protocol as defined by the MEF 16 standard, defines the use of only two message types—STATUS ENQUIRY and STATUS.

These E-LMI messages consist of required and optional fields called information elements, and all information elements are associated with assigned identifiers. All messages contain the Protocol Version, Message Type, and Report Type information elements, followed by optional information elements and sub-information elements.

E-LMI messages are encapsulated in 46- to 1500-byte Ethernet frames, which are based on the IEEE 802.3 untagged MAC-frame format. E-LMI frames consist of the following fields:

- Destination address (6 bytes)—Uses a standard MAC address of 01:80:C2:00:00:07.
- Source address (6 bytes)—MAC address of the sending device or port.

- E-LMI Ethertype (2 bytes)—Uses 88-EE.
- E-LMI PDU (46–1500 bytes)—Data plus 0x00 padding as needed to fulfill minimum 46-byte length.
- CRC (4 bytes)—Cyclic Redundancy Check for error detection.

Cisco-Proprietary Remote UNI Details Information Element

The E-LMI MEF 16 specification does not define a way to send proprietary information.

To provide additional information within the E-LMI protocol, the Cisco IOS XR software implements a Cisco-proprietary information element called Remote UNI Details to send information to the CE about remote UNI names and states. This information element implements what is currently an unused identifier from the E-LMI MEF 16 specification.

To ensure compatibility for future implementations of E-LMI should this identifier ever be implemented in the standard protocol, or for another reason, you can disable transmission of the Remote UNI information element using the **extension remote-uni disable** command.

E-LMI Operation

The basic operation of E-LMI consists of a CE device sending periodic STATUS ENQUIRY messages to the PE device, followed by mandatory STATUS message responses by the PE device that contain the requested information. Sequence numbers are used to correlate STATUS ENQUIRY and STATUS messages between the CE and PE.

The CE sends the following two forms of STATUS ENQUIRY messages called Report Types:

- E-LMI Check—Verifies a Data Instance (DI) number with the PE to confirm that the CE has the latest E-LMI information.
- Full Status—Requests information from the PE about the UNI and all EVCs.

The CE device uses a polling timer to track sending of STATUS ENQUIRY messages, while the PE device can optionally use a Polling Verification Timer (PVT), which specifies the allowable time between transmission of the PE’s STATUS message and receipt of a STATUS ENQUIRY from the CE device before recording an error.

In addition to the periodic STATUS ENQUIRY/STATUS message sequence for the exchange of E-LMI information, the PE device also can send asynchronous STATUS messages to the CE device to communicate changes in EVC status as soon as they occur and without any prompt by the CE device to send that information.

Both the CE and PE devices use a status counter (N393) to determine the local operational status of E-LMI by tracking consecutive errors received before declaring a change in E-LMI protocol status.

Supported E-LMI PE Functions

The Cisco NCS 4000 Series Router serves as the PE device for E-LMI on a MEN, and supports the following PE functions:

- Supports the E-LMI protocol on Ethernet physical interfaces that are configured with Layer 2 subinterfaces as Ethernet Flow Points (EFPs), which serve as the EVCs about which the physical interface reports status to the CE. The Cisco IOS XR software does not support a specific manageability context for an Ethernet Virtual Connection (EVC).

Note For E-LMI on the Cisco NCS 4000 Series Router, the term EVC in this documentation refers to a Layer 2 subinterface/EFP.

- Provides the ability to configure the following E-LMI options defined in the MEF 16 specification:
  - T392 Polling Verification Timer (PVT)
  - N393 Status Counter
- Sends notification of the addition and deletion of an EVC.
- Sends notification of the availability (active) or unavailability (inactive, partially active) status of a configured EVC.
- Sends notification of the local UNI name.
- Sends notification of remote UNI names and states using the Cisco-proprietary Remote UNI Details information element, and the ability to disable the Cisco-proprietary Remote UNI information element.
- Sends information about UNI and EVC attributes to the CE (to allow the CE to auto-configure these attributes), including:
  - CE-VLAN to EVC Map
  - CE-VLAN Map Type (Bundling, All-to-one Bundling, Service Multiplexing)
  - Service Type (point-to-point or multipoint)
- Uses CFM Up MEPs to retrieve the EVC state, EVC Service Type, and remote UNI details.
- Provides the ability to retrieve the per-interface operational state of the protocol (including all the information currently being communicated by the protocol to the CE) using the command-line interface (CLI) or Extensible Markup Language (XML) interface.
- Supports up to 80 E-LMI sessions per linecard (one per physical interface).
- Supports up to 32000 EVCs total per linecard for all physical interfaces enabled for E-LMI.

How to Configure Ethernet OAM

This section provides these configuration procedures:

Configuring Ethernet Link OAM

Custom EOAM settings can be configured and shared on multiple interfaces by creating an EOAM profile in Ethernet configuration mode and then attaching the profile to individual interfaces. The profile configuration does not take effect until the profile is attached to an interface. After an EOAM profile is attached to an interface, individual EOAM features can be configured separately on the interface to override the profile settings when desired.

This section describes how to configure an EOAM profile and attach it to an interface in these procedures:

Configuring an Ethernet OAM Profile

Perform these steps to configure an Ethernet OAM profile.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure terminal
```

Enters global configuration mode.

Step 2 **ethernet oam profile** *profile-name*

Example:

```
RP/0/RP0:hostname(config)# ethernet oam profile Profile_1
```

Creates a new Ethernet Operations, Administration and Maintenance (OAM) profile and enters Ethernet OAM configuration mode.

Step 3 **link-monitor**

Example:

```
RP/0/RP0:hostname(config-eoam)# link-monitor
```

Enters the Ethernet OAM link monitor configuration mode.

Step 4 **symbol-period window** *window*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# symbol-period window 60000
```

(Optional) Configures the window size (in milliseconds) for an Ethernet OAM symbol-period error event.

The range is 1000 to 60000.

The default value is 1000.

Step 5 **symbol-period threshold low** *threshold* **high** *threshold*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# symbol-period threshold low 10000000 high 60000000
```

(Optional) Configures the thresholds (in symbols) that trigger an Ethernet OAM symbol-period error event. The high threshold is optional and is configurable only in conjunction with the low threshold.

The range is 0 to 60000000.

The default low threshold is 1.

Step 6 **frame window** *window*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# frame window 60
```

(Optional) Configures the frame window size (in milliseconds) of an OAM frame error event.

The range is from 1000 to 60000.

The default value is 1000.

Step 7 **frame threshold low** *threshold* **high** *threshold*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# frame threshold low 10000000 high 60000000
```

(Optional) Configures the thresholds (in symbols) that triggers an Ethernet OAM frame error event. The high threshold is optional and is configurable only in conjunction with the low threshold.

The range is from 0 to 60000000.

The default low threshold is 1.

Step 8 **frame-period window** *window*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# frame-period window 60000
```

(Optional) Configures the window size (in milliseconds) for an Ethernet OAM frame-period error event.

The range is from 100 to 60000.

The default value is 1000.

Step 9 **frame-period threshold low** *threshold* **high** *threshold*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# frame threshold low 10000000 high 60000000
```

(Optional) Configures the thresholds (in frames) that trigger an Ethernet OAM frame-period error event. The high threshold is optional and is configurable only in conjunction with the low threshold.

The range is 0 to 1000000.

The default low threshold is 60000.

Step 10 **frame-seconds window** *window*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# frame-seconds window 900000
```

(Optional) Configures the window size (in milliseconds) for the OAM frame-seconds error event.

The range is 10000 to 900000.

The default value is 6000.

Step 11 **frame-seconds threshold low** *threshold* **high** *threshold*

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# frame-seconds threshold 3 threshold 900
```

(Optional) Configures the thresholds (in seconds) that trigger a frame-seconds error event. The high threshold value can be configured only in conjunction with the low threshold value.

The range is 1 to 900

The default value is 1.

Step 12 **exit**

Example:

```
RP/0/RP0:hostname(config-eoam-lm)# exit
```

Exits back to Ethernet OAM mode.

Step 13 **mib-retrieval**

Example:

```
RP/0/RP0:hostname(config-eoam)# mib-retrieval
```

Enables MIB retrieval in an Ethernet OAM profile or on an Ethernet OAM interface.

Step 14 **connection timeout** <*timeout*>

Example:

```
RP/0/RP0:hostname(config-eoam)# connection timeout 30
```

Configures the connection timeout period for an Ethernet OAM session. as a multiple of the hello interval.

The range is 2 to 30.

The default value is 5.

Step 15 **hello-interval** {**100ms**|**1s**}

Example:

```
RP/0/RP0:hostname(config-eoam)# hello-interval 100ms
```

Configures the time interval between hello packets for an Ethernet OAM session. The default is 1 second (**1s**).

Step 16 **mode** {**active**|**passive**}

Example:

```
RP/0/RP0:hostname(config-eoam)# mode passive
```

Configures the Ethernet OAM mode. The default is active.

Step 17 **require-remote mode** {**active**|**passive**}

Example:

```
RP/0/RP0:hostname(config-eoam)# require-remote mode active
```

Requires that active mode or passive mode is configured on the remote end before the OAM session becomes active.

Step 18 **require-remote link-monitoring**

Example:

```
RP/0/RP0:hostname(config-eoam)# require-remote link-monitoring
```

Requires that link-monitoring is configured on the remote end before the OAM session becomes active.

Step 19 **require-remote mib-retrieval**

Example:

```
RP/0/RP0:hostname(config-eoam)# require-remote mib-retrieval
```

Requires that MIB-retrieval is configured on the remote end before the OAM session becomes active.

Step 20 **action capabilities-conflict** {**disable** | **efd** | **error-disable-interface**}

Example:

```
RP/0/RP0:hostname(config-eoam)# action capabilities-conflict efd
```

Specifies the action that is taken on an interface when a capabilities-conflict event occurs. The default action is to create a syslog entry.

Note
- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 21 **action critical-event** {**disable** | **error-disable-interface**}

Example:

```
RP/0/RP0:hostname(config-eoam)# action critical-event error-disable-interface
```

Specifies the action that is taken on an interface when a critical-event notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.

Note
- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 22 **action discovery-timeout** {**disable** | **efd** | **error-disable-interface**}

Example:

```
RP/0/RP0:hostname(config-eoam)# action discovery-timeout efd
```

Specifies the action that is taken on an interface when a connection timeout occurs. The default action is to create a syslog entry.

Note
- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 23 **action dying-gasp** {**disable** | **error-disable-interface**}

Example:

```
RP/0/RP0:hostname(config-eoam)# action dying-gasp error-disable-interface
```

Specifies the action that is taken on an interface when a dying-gasp notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.

Note

- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 24 **action high-threshold** {**error-disable-interface** | **log**}

Example:

```
RP/0/RP0:hostname(config-eoam)# action high-threshold error-disable-interface
```

Specifies the action that is taken on an interface when a high threshold is exceeded. The default is to take no action when a high threshold is exceeded.

Note

- If you change the default, the **disable** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and take no action at the interface when the event occurs.

Step 25 **action remote-loopback disable**

Example:

```
RP/0/RP0:hostname(config-eoam)# action remote-loopback disable
```

Specifies that no action is taken on an interface when a remote-loopback event occurs. The default action is to create a syslog entry.

Note

- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 26 **action session-down** {**disable** | **efd** | **error-disable-interface**}

Example:

```
RP/0/RP0:hostname(config-eoam)# action session-down efd
```

Specifies the action that is taken on an interface when an Ethernet OAM session goes down.

Note

- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 27 **action session-up disable**

Example:

```
RP/0/RP0:hostname(config-eoam)# action session-up disable
```

Specifies that no action is taken on an interface when an Ethernet OAM session is established. The default action is to create a syslog entry.

Note
- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 28 **action uni-directional link-fault** {**disable** | **efd** | **error-disable-interface**}

Specifies the action that is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer. The default action is to create a syslog entry.

Note
- If you change the default, the **log** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.

Step 29 **action wiring-conflict** {**disable** | **efd** | **log**}

Example:

```
RP/0/RP0:hostname(config-eoam)# action session-down efd
```

Specifies the action that is taken on an interface when a wiring-conflict event occurs. The default is to put the interface into error-disable state.

Note
- If you change the default, the **error-disable-interface** keyword option is available in Interface Ethernet OAM configuration mode to override the profile setting and put the interface into error-disable state when the event occurs.

Step 30 **uni-directional link-fault detection**

Example:

```
RP/0/RP0:hostname(config-eoam)# uni-directional link-fault detection
```

Enables detection of a local, unidirectional link fault and sends notification of that fault to an Ethernet OAM peer.

Step 31 **commit**

Example:

```
RP/0/RP0:hostname(config-if)# commit
```

Saves the configuration changes to the running configuration file and remains within the configuration session.

Step 32 **end**

Example:

```
RP/0/RP0:hostname(config-if)# end
```

Ends the configuration session and exits to the EXEC mode.

Attaching an Ethernet OAM Profile to an Interface

Perform these steps to attach an Ethernet OAM profile to an interface:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure terminal
```

Enters global configuration mode.

Step 2 **interface** [**FastEthernet** | **HundredGigE**| **TenGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface
TenGigE 0/1/0/0
```

Enters interface configuration mode and specifies the Ethernet interface name and notation *rack/slot/module/port*.

Note • The example indicates an 8-port 10-Gigabit Ethernet interface in modular services card slot 1.

Step 3 **ethernet oam**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet oam
```

Enables Ethernet OAM and enters interface Ethernet OAM configuration mode.

Step 4 **profile** *profile-name*

Example:

```
RP/0/RP0:hostname(config-if-eoam)# profile Profile_1
```

Attaches the specified Ethernet OAM profile (*profile-name*), and all of its configuration, to the interface.

Step 5 **commit**

Example:

```
RP/0/RP0:hostname(config-if)# commit
```

Saves the configuration changes to the running configuration file and remains within the configuration session.

Step 6 **end**

Example:

```
RP/0/RP0:hostname(config-if)# end
```

Ends the configuration session and exits to the EXEC mode.

Configuring Ethernet OAM at an Interface and Overriding the Profile Configuration

Using an EOAM profile is an efficient way of configuring multiple interfaces with a common EOAM configuration. However, if you want to use a profile but also change the behavior of certain functions for a particular interface, then you can override the profile configuration. To override certain profile settings that are applied to an interface, you can configure that command in interface Ethernet OAM configuration mode to change the behavior for that interface.

In some cases, only certain keyword options are available in interface Ethernet OAM configuration due to the default settings for the command. For example, without any configuration of the **action** commands, several forms of the command have a default behavior of creating a syslog entry when a profile is created and applied to an interface. Therefore, the **log** keyword is not available in Ethernet OAM configuration for these commands in the profile because it is the default behavior. However, the **log** keyword is available in Interface Ethernet OAM configuration if the default is changed in the profile configuration so you can retain the action of creating a syslog entry for a particular interface.

To see all of the default Ethernet OAM configuration settings, see the Verifying the Ethernet OAM Configuration.

To configure Ethernet OAM settings at an interface and override the profile configuration, perform these steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure terminal
```

Enters global configuration mode.

Step 2 **interface** [TenGigE | HundredGigE] *interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/0
```

Enters interface configuration mode and specifies the Ethernet interface name and notation *rack/slot/module/port*.

Step 3 **ethernet oam**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet oam
```

Enables Ethernet OAM and enters interface Ethernet OAM configuration mode.

Step 4 *interface-Ethernet-OAM-command*

Example:

```
RP/0/RP0:hostname(config-if-eoam)# action capabilities-conflict error-disable-interface
```

Configures a setting for an Ethernet OAM configuration command and overrides the setting for the profile configuration, where *interface-Ethernet-OAM-command* is one of the supported commands on the platform in interface Ethernet OAM configuration mode.

Step 5 **commit**

Example:

```
RP/0/RP0:hostname(config-if)# commit
```

Saves the configuration changes to the running configuration file and remains within the configuration session.

Step 6 **end**

Example:

```
RP/0/RP0:hostname(config-if)# end
```

Ends the configuration session and exits to the EXEC mode.

Verifying the Ethernet OAM Configuration

Use the **show ethernet oam configuration** command to display the values for the Ethernet OAM configuration for a particular interface, or for all interfaces. The following example shows the default values for Ethernet OAM settings:

```
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:                                      Y
  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
```

Configuring Ethernet CFM

To configure Ethernet CFM, perform the following tasks:

Configuring Cross-Check on a MEP for a CFM Service

To configure cross-check on a MEP for a CFM service and specify the expected set of MEPs, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname# ethernet cfm
```

Enters the Ethernet Connectivity Fault Management (CFM) configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Creates and names a container for all domain configurations and enters the CFM domain configuration mode.

The level must be specified.

The **id** is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames.

Step 4 **service** *service-name* [**down-meps** | **xconnect**] **id** [**icc-based** *icc-string* | **number** *number*]

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# service Bridge_Service down-meps number 10
```

Configures and associates a service with the domain and enters CFM domain service configuration mode.

The **id** sets the short MA name.

Step 5 **mep crosscheck**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# mep crosscheck mep-id 10
```

Enters CFM MEP crosscheck configuration mode.

Step 6 **mep-id** *mep-id-number* [**mac-address** *mac-address*]

Example:

```
RP/0/RP0:hostname(config-cfm-xcheck)# mep-id 10
```

Enables cross-check on a MEP.

Note
- Repeat this command for every MEP that you want included in the expected set of MEPs for cross-check.

Step 7 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-cfm-xcheck)# commit
```

Saves configuration changes.

Configuring a CFM Maintenance Domain

To configure a CFM maintenance domain, perform the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config)# ethernet cfm
```

Enters Ethernet Connectivity Fault Management (CFM) configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Creates and names a container for all domain configurations and enters CFM domain configuration mode.

The level must be specified.

The **id** is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames.

Step 4 **traceroute cache hold-time** *minutes* **size** *entries*

Example:

```
RP/0/RP0:hostname(config-cfm)# traceroute cache hold-time 1 size 3000
```

(Optional) Sets the maximum limit of traceroute cache entries or the maximum time limit to hold the traceroute cache entries. The default is 100 minutes and 100 entries.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# commit
```

Saves configuration changes.

Configuring Services for a CFM Maintenance Domain

You can configure up to 32000 CFM services for a maintenance domain.

Before you begin

To configure services for a CFM maintenance domain, perform the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config)# ethernet cfm
```

Enters Ethernet CFM configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Creates and names a container for all domain configurations at a specified maintenance level, and enters CFM domain configuration mode.

The **id** is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames.

Step 4 **service** *service-name* [**down-meps** | **xconnect**] **id** [**icc-based** *icc-string* | **number** *number*]

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# service Bridge_Service down-meps number 10
```

Configures and associates a service with the domain and enters CFM domain service configuration mode.

The **id** sets the short MA name.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# commit
```

Saves configuration changes.

Enabling and Configuring Continuity Check for a CFM Service

It supports Continuity Check as defined in the IEEE 802.1ag specification, and supports CCMs intervals of 100 ms and longer. The overall packet rates for CCM messages are up to 16000 CCMs-per-second sent, and up to 16000 CCMs-per-second received, per card.

Note If Ethernet SLA is configured, the overall combined packet rate for CCMs and SLA frames is 16000 frames-per-second in each direction, per card.

To configure Continuity Check for a CFM service, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config)# ethernet cfm
```

Enters Ethernet Connectivity Fault Management (CFM) configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Creates and names a container for all domain configurations and enters the CFM domain configuration mode.

The level must be specified.

The **id** is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames.

Step 4 **service** *service-name* [**down-meps** | **xconnect**] **id** [**icc-based** *icc-string* | **number** *number*]

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# service Bridge_Service down-meps number 10
```

Configures and associates a service with the domain and enters CFM domain service configuration mode.

The **id** sets the short MA name.

Step 5 **continuity-check interval** *time* [**loss-threshold** *threshold*]

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# continuity-check interval 100m loss-threshold 10
```

(Optional) Enables Continuity Check and specifies the time interval at which CCMs are transmitted or to set the threshold limit for when a MEP is declared down.

Step 6 **continuity-check archive hold-time** *minutes*

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# continuity-check archive hold-time 100
```

(Optional) Configures how long information about peer MEPs is stored after they have timed out.

Step 7 **continuity-check loss auto-traceroute**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# continuity-check loss auto-traceroute
```

(Optional) Configures automatic triggering of a traceroute when a MEP is declared down.

Step 8 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# commit
```

Saves configuration changes.

Configuring Automatic MIP Creation for a CFM Service

To configure automatic MIP creation for a CFM service, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname# ethernet cfm
```

Enters the Ethernet Connectivity Fault Management (CFM) configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Creates and names a container for all domain configurations at a specified maintenance level, and enters CFM domain configuration mode.

The **id** is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames.

Step 4 **service** *service-name* [**down-meps** | **xconnect**] **id** [**icc-based** *icc-string* | **number** *number*]

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# service Bridge_Service down-meps number 10
```

Configures and associates a service with the domain and enters CFM domain service configuration mode.

The **id** sets the short MA name.

Step 5 **mip auto-create** {**all** | **lower-mep-only**}

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# mip auto-create all
```

(Optional) Enables the automatic creation of MIPs in a bridge domain or xconnect.

Step 6 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# commit
```

Saves configuration changes.

Configuring Other Options for a CFM Service

To configure other options for a CFM service, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config)# ethernet cfm
```

Enters the Ethernet Connectivity Fault Management (CFM) configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Creates and names a container for all domain configurations and enters the CFM domain configuration mode.

The level must be specified.

The **id** is the maintenance domain identifier (MDID) and is used as the first part of the maintenance association identifier (MAID) in CFM frames.

Step 4 **service** *service-name* [**down-meps** | **xconnect**] **id** [**icc-based** *icc-string* | **number** *number*]

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# service Bridge_Service down-meps number 10
```

Configures and associates a service with the domain and enters CFM domain service configuration mode.

The **id** sets the short MA name.

Step 5 **maximum-meps** *number*

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# maximum-meps 1000
```

(Optional) Configures the maximum number (2 to 8190) of MEPs across the network, which limits the number of peer MEPs recorded in the database.

Step 6 **log** {**ais**|**continuity-check errors**|**continuity-check mep changes**|**crosscheck errors**|**efd**}

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# log continuity-check errors
```

(Optional) Enables logging of certain types of events.

Step 7 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# commit
```

Saves configuration changes.

Configuring CFM MEPs

When you configure CFM MEPs, consider these guidelines:

- Up to 1000 local MEPs are supported per card.
- CFM maintenance points can be created on All physical Ethernet interfaces (except for the RP Management interfaces).
- CFM maintenance points can be created on both Layer 2 interfaces.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** { **TenGigE | HundredGigE**} *interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/1
```

Type of Ethernet interface on which you want to create a MEP. Enter **TenGigE** or **HundredGigE** and the 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.

Step 3 **interface** { **TenGigE | HundredGigE | Bundle-Ether**} *interface-path-id***.***subinterface*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/1
```

Type of Ethernet interface on which you want to create a MEP. Enter **TenGigE, HundredGigE** or **Bundle-Ether** and the physical interface or virtual interface followed by the subinterface path ID.

Naming notation is *interface-path-id***.***subinterface*. The period in front of the subinterface value is required as part of the notation.

For more information about the syntax for the router, use the question mark (**?**) online help function.

Step 4 **interface** {**FastEthernet | TenGigE | HundredGigE**} *interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/1
```

Type of Ethernet interface on which you want to create a MEP. Enter **FastEthernet, TenGigE** or **HundredGigE** and the 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.

Step 5 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet cfm
```

Enters interface Ethernet CFM configuration mode.

Step 6 **mep domain** *domain-name* **service** *service-name* **mep-id** *id-number*

Example:

```
RP/0/RP0:hostname(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
```

Creates a maintenance end point (MEP) on an interface and enters interface CFM MEP configuration mode.

Step 7 **cos** *cos*

Example:

```
RP/0/RP0:hostname(config-if-cfm-mep)# cos 7
```

(Optional) Configures the class of service (CoS) (from 0 to 7) for all CFM packets generated by the MEP on an interface. If not configured, the CoS is inherited from the Ethernet interface.

Step 8 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if-cfm-mep)# commit
```

Configuring Y.1731 AIS

This section has the following step procedures:

Configuring AIS in a CFM Domain Service

Use the following procedure to configure Alarm Indication Signal (AIS) transmission for a CFM domain service and configure AIS logging.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config)# ethernet cfm
```

Enters Ethernet CFM global configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Specifies the domain and domain level.

Step 4 **service** *name* **xconnect group** *xconnect-group-name* **p2p** *xconnect-name*

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# service S1 bridge group BG1 bridge-domain BD2
```

Specifies the service and cross-connect group and name.

Step 5 **ais transmission** [**interval** {**1s**|**1m**}][**cos** *cos*]

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# ais transmission interval 1m cos 7
```

Configures Alarm Indication Signal (AIS) transmission for a Connectivity Fault Management (CFM) domain service.

Step 6 **log ais**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# log ais
```

Configures AIS logging for a Connectivity Fault Management (CFM) domain service to indicate when AIS or LCK packets are received.

Step 7 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-sla-prof-stat-cfg)# commit
```

Saves configuration changes.

Configuring AIS on a CFM Interface

To configure AIS on a CFM interface, perform the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface TenGigE** *interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/2
```

Enters interface configuration mode.

Step 3 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet cfm
```

Enters Ethernet CFM interface configuration mode.

Step 4 **ais transmission up interval 1m cos** *cos*

Example:

```
RP/0/RP0:hostname(config-if-cfm)# ais transmission up interval 1m cos 7
```

Configures Alarm Indication Signal (AIS) transmission on a Connectivity Fault Management (CFM) interface.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if-cfm)# commit
```

Saves configuration changes.

Configuring EFD for a CFM Service

To configure EFD for a CFM service, complete the following steps.

Restrictions

EFD is not supported on up MEPs. It can only be configured on down MEPs, within a particular service.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **ethernet cfm**

Example:

```
RP/0/RP0:hostname(config)# ethernet cfm
```

Enters CFM configuration mode.

Step 3 **domain** *domain-name* **level** *level-value* **id null**

Example:

```
RP/0/RP0:hostname(config-cfm)# domain Domain_One level 1 id null
```

Specifies or creates the CFM domain and enters CFM domain configuration mode.

Step 4 **service** *service-name* **down-meps**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn)# service S1 down-meps
```

Specifies or creates the CFM service for down MEPS and enters CFM domain service configuration mode.

Step 5 **efd**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# efd
```

Enables EFD on all down MEPs in the down MEPS service.

Step 6 **log efd**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# log efd
```

(Optional) Enables logging of EFD state changes on an interface.

Step 7 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# commit
```

Saves configuration changes.

Verifying the EFD Configuration

This 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
```

Verifying the CFM Configuration

To verify the CFM configuration, use one or more of the following commands:

show ethernet cfm configuration-errors [**domain** *domain-name*] [**interface** *interface-path-id*]	Displays information about errors that are preventing configured CFM operations from becoming active, as well as any warnings that have occurred.
show ethernet cfm local maintenance-points domain *name* [**service** *name]* | **interface** *type interface-path-id*] [**mep** | **mip**]	Displays a list of local maintenance points.

Troubleshooting Tips

To troubleshoot problems within the CFM network, perform the following steps:

Procedure

Step 1 To verify connectivity to a problematic MEP, use the **ping ethernet cfm** command as shown in the following example:

```
RP/0/RP0:hostname# ping ethernet cfm domain D1 service S1 mep-id 16 source
interface TenGigE  0/0/0/0

Type escape sequence to abort.
Sending 5 CFM Loopbacks, timeout is 2 seconds -
Domain foo (level 2), Service foo
Source: MEP ID 1, interface TenGigE0/0/0/0
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
```

Step 2 If the results of the **ping ethernet cfm** command show a problem with connectivity to the peer MEP, use the **traceroute ethernet cfm** command to help further isolate the location of the problem as shown in the following example:

```
RP/0/RP0:hostname# traceroute ethernet cfm domain D1 service S1 mep-id 16
source interface TenGigE 0/0/0/0

Traceroutes in domain D1 (level 4), service S1
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    TenGigE0/0/0/0
  2 abc                                             0001.0203.0401 [Ok]    FDB
      ios                                           Not present
  3 bcd                      0001.0203.0402 [Ok]                           Hit
      abc                    TenGigE0/0
Replies dropped: 0
```

If the target was a MEP, verify that the last hop shows “Hit” in the Relay field to confirm connectivity to the peer MEP.

If the Relay field contains “MPDB” for any of the hops, then the target MAC address was not found in the bridge MAC learning table at that hop, and the result is relying on CCM learning. This result can occur under normal conditions, but it can also indicate a problem. If you used the **ping ethernet cfm** command before using the **traceroute ethernet cfm** command, then the MAC address should have been learned. If “MPDB” is appearing in that case, then this indicates a problem at that point in the network.

Configuring Ethernet LMI

To configure Ethernet LMI, complete the following tasks:

Prerequisites for Configuring E-LMI

Before you configure E-LMI on the Cisco NCS 4000 Series Router, be sure that you complete the following requirements:

- Identify the local and remote UNIs in your network where you want to run E-LMI, and define a naming convention for them.
- Enable E-LMI on the corresponding CE interface link on a device that supports E-LMI CE operation, such as the Cisco Catalyst 3750 Metro Series Switches.

Restrictions for Configuring E-LMI

When configuring E-LMI, consider the following restrictions:

- E-LMI is not supported on subinterfaces or bundle interfaces. E-LMI is configurable on Ethernet physical interfaces only.

Configuring UNI Names on the Physical Interface

It is recommended that you configure UNI names on the physical interface links to both the local and remote UNIs to aid in management for the E-LMI protocol. To configure UNI names, complete the following tasks on the physical interface links to both the local and remote UNIs:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface [TenGigE | HundredGigE]** *interface-path-id*

Example:

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

Enters interface configuration mode for the physical interface.

Step 3 **ethernet uni id** *name*

Example:

```
RP/0/RP0:hostname(config-if)# ethernet uni id PE1-CustA-Slot0-Port0
```

Specifies a name (up to 64 characters) for the Ethernet UNI interface link.

Step 4 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if)# commit
```

Saves configuration changes.

Enabling E-LMI on the Physical Interface

It supports the E-LMI protocol only on physical Ethernet interfaces. To enable E-LMI, complete the following tasks on the physical Ethernet interface link to the local UNI:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE** | **HundredGigE**] *interface-path-id*

Example:

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

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet lmi
```

Enables Ethernet Local Management Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if-lmi)# commit
```

Saves configuration changes.

Configuring the Status Counter

The MEF N393 Status Counter value is used to determine E-LMI operational status by tracking receipt of consecutive good packets or successive expiration of the PVT on packets. The default counter is four, which means that while the E-LMI protocol is in Down state, four good packets must be received consecutively to change the protocol state to Up, or while the E-LMI protocol is in Up state, four consecutive PVT expirations must occur before the state of the E-LMI protocol is changed to Down on the interface.

To modify the status counter default value, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE** | **HundredGigE**] *interface-path-id*

Example:

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

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **status-counter** *threshold*

Example:

```
RP/0/RP0:hostname(config-if-lmi)# status-counter 5
```

Sets the MEF N393 Status Counter value that is used to determine E-LMI operational status by tracking receipt of consecutive good and bad packets from a peer. The default is 4.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if-lmi)# commit
```

Saves configuration changes.

Configuring the Polling Verification Timer

The MEF T392 Polling Verification Timer (PVT) specifies the allowable time between transmission of a STATUS message and receipt of a STATUS ENQUIRY from the UNI-C before recording an error. The default value is 15 seconds.

To modify the default value or disable the PVT altogether, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE** | **HundredGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname# interface TenGigE 0/0/0/0
```

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **polling-verification-timer** {*interval* | **disable**}

Example:

```
RP/0/RP0:hostname(config-if-lmi)# polling-verification-timer 30
```

Sets or disables the MEF T392 Polling Verification Timer for E-LMI operation, which specifies the allowable time (in seconds) between transmission of a STATUS message and receipt of a STATUS ENQUIRY from the UNI-C before recording an error. The default is 15.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if-lmi)# commit
```

Saves configuration changes.

Disabling Syslog Messages for E-LMI Errors or Events

The E-LMI protocol tracks certain errors and events whose counts can be displayed using the **show ethernet lmi interfaces** command.

To disable syslog messages for E-LMI errors or events, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE** | **HundredGigE**] *interface-path-id*

Example:

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

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **log** {**errors** | **events**} **disable**

Example:

```
RP/0/RP0:hostname(config-if-lmi)# log events disable
```

Turns off syslog messages for E-LMI errors or events.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if-lmi)# commit
```

Saves configuration changes.

Disabling Use of the Cisco-Proprietary Remote UNI Details Information Element

To provide additional information within the E-LMI protocol, the Cisco IOS XR software implements a Cisco-proprietary information element called Remote UNI Details to send information to the CE about remote UNI names and states. This information element implements what is currently an unused identifier from the E-LMI MEF 16 specification.

To disable use of the Remote UNI Details information element, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE** | **HundredGigE**] *interface-path-id*

Example:

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

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **extension remote-uni disable**

Example:

```
RP/0/RP0:hostname(config-if-lmi)# extension remote-uni disable
```

Disables transmission of the Cisco-proprietary Remote UNI Details information element in E-LMI STATUS messages.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname(config-if-lmi)# commit
```

Saves configuration changes.

Verifying the Ethernet LMI Configuration

Use the **show ethernet lmi interfaces detail** command to display the values for the Ethernet LMI configuration for a particular interface, or for all interfaces. The following example shows sample output for 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-Slot0-Port0
  Line Protocol State: Up
  MTU: 1514 (1 PDU 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: 0
  Last Sequence Numbers: Sent 0, Received 0

  Reliability Errors:
    Status Enq Timeouts                  0 Invalid Sequence Number             0
    Invalid Report Type                  0

  Protocol Errors:
    Malformed PDUs                       0 Invalid Procotol 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 Received     never       Full Status Sent         never
  PDU Received                 never       PDU Sent                 never
  LMI Link Status Changed   00:00:03 ago   Last Protocol Error      never
  Counters cleared             never

  Sub-interface: TenGigE0/0/0/0.0
    VLANs: 1-20
    EVC Status: Active
    EVC Type: Point-to-Point
    OAM Protocol: CFM
      CFM Domain: Global (level 5)
      CFM Service: CustomerA
    Remote UNI Count: Configured = 1, Active = 1

    Remote UNI Id                                                 Status
    -------------                                                 ------
    PE1-CustA-Slot0-Port1                                         Up
```

Configuration Examples for Ethernet OAM

This section provides the following configuration examples:

Configuration Examples for EOAM Interfaces

This section provides the following configuration examples:

Configuring an Ethernet OAM Profile Globally: Example

This example shows how to configure an Ethernet OAM profile globally:

```
configure terminal
 ethernet oam profile Profile_1
  link-monitor
   symbol-period window 60000
   symbol-period threshold low 10000000 high 60000000
   frame window 60
   frame threshold low 10000000 high 60000000
   frame-period window 60000
   frame-period threshold low 100 high 12000000
   frame-seconds window 900000
   frame-seconds threshold 3 threshold 900
   exit
  mib-retrieval
  connection timeout 30
  require-remote mode active
  require-remote link-monitoring
  require-remote mib-retrieval
  action dying-gasp error-disable-interface
  action critical-event error-disable-interface
  action discovery-timeout error-disable-interface
  action session-down error-disable-interface
  action capabilities-conflict error-disable-interface
  action wiring-conflict error-disable-interface
  action remote-loopback error-disable-interface
  commit
```

Configuring Ethernet OAM Features on an Individual Interface: Example

This example shows how to configure Ethernet OAM features on an individual interface:

```
configure terminal
 interface TenGigE 0/1/0/0
  ethernet oam
   link-monitor
    symbol-period window 60000
    symbol-period threshold low 10000000 high 60000000
    frame window 60
    frame threshold low 10000000 high 60000000
    frame-period window 60000
    frame-period threshold low 100 high 12000000
    frame-seconds window 900000
    frame-seconds threshold 3 threshold 900
    exit
   mib-retrieval
   connection timeout 30
   require-remote mode active
   require-remote link-monitoring
   require-remote mib-retrieval
   action link-fault  error-disable-interface
   action dying-gasp error-disable-interface
   action critical-event error-disable-interface
   action discovery-timeout error-disable-interface
   action session-down error-disable-interface
   action capabilities-conflict error-disable-interface
   action wiring-conflict error-disable-interface
   action remote-loopback error-disable-interface
   commit
```

Configuring Ethernet OAM Features to Override the Profile on an Individual Interface: Example

This example shows the configuration of Ethernet OAM features in a profile followed by an override of that configuration on an interface:

```
configure terminal
 ethernet oam profile Profile_1
  mode passive
  action dying-gasp disable
  action critical-event disable
  action discovery-timeout disable
  action session-up disable
  action session-down disable
  action capabilities-conflict disable
  action wiring-conflict disable
  action remote-loopback disable
  action uni-directional link-fault error-disable-interface
  commit

configure terminal
 interface TenGigE 0/1/0/0
  ethernet oam
   profile Profile_1
    mode active
    action dying-gasp log
    action critical-event log
    action discovery-timeout log
    action session-up log
    action session-down log
    action capabilities-conflict log
    action wiring-conflict log
    action remote-loopback log
    action uni-directional link-fault log
    uni-directional link-fault detection
    commit
```

Configuring a Remote Loopback on an Ethernet OAM Peer: Example

This example shows how to configure a remote loopback on an Ethernet OAM peer:

```
RP/0/RP0:hostname# configure terminal
RP/0/RP0:hostname(config)# interface TenGigE 0/1/5/6
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)# remote-loopback
RP/0/RP0:hostname(config-if-eoam)# commit
```

This example shows how to start a remote loopback on a configured Ethernet OAM interface:

```
RP/0/RP0:hostname# ethernet oam loopback enable TenGigE 0/1/5/6
```

Clearing Ethernet OAM Statistics on an Interface: Example

This example shows how to clear Ethernet OAM statistics on an interface:

```
RP/0/RP0:hostname# clear ethernet oam statistics interface TenGigE 0/1/5/1
```

Enabling SNMP Server Traps on a Router: Example

This example shows how to enable SNMP server traps on a router:

```
configure terminal
  ethernet oam profile Profile_1
  snmp-server traps ethernet oam events
```

Configuration Examples for Ethernet CFM

This section includes the following examples:

Ethernet CFM Domain Configuration: Example

This example shows how to configure a basic domain for Ethernet CFM:

```
  configure
  ethernet cfm
  traceroute cache hold-time 1 size 3000
  domain Domain_One level 1 id null
  commit
```

Ethernet CFM Service Configuration: Example

The following examples show how to create a service for an Ethernet CFM Service:

```
 RP/0/RP0:hostname(config-cfm-dmn)# service Bridge_Service down-meps number 10
 RP/0/RP0:hostname(config-cfm-dmn)# commit
```

```
 RP/0/RP0:hostname(config-cfm-dmn)# service S1 xconnect group XG1 p2p X1
 RP/0/RP0:hostname(config-cfm-dmn)# commit
```

Continuity Check for an Ethernet CFM Service Configuration: Example

This example shows how to configure continuity-check options for an Ethernet CFM service:

```
   continuity-check archive hold-time 100
   continuity-check loss auto-traceroute
   continuity-check interval 100ms loss-threshold 10
   commit
```

MIP Creation for an Ethernet CFM Service Configuration: Example

This example shows how to enable MIP auto-creation for an Ethernet CFM service:

```
RP/0/RP0:hostname(config-cfm-dmn-svc)# mip auto-create all
RP/0/RP0:hostname(config-cfm-dmn-svc)# commit
```

Cross-check for an Ethernet CFM Service Configuration: Example

This example shows how to configure cross-check for MEPs in an Ethernet CFM service:

```
   mep crosscheck
    mep-id 10
    mep-id 20
    commit
```

Other Ethernet CFM Service Parameter Configuration: Example

This example shows how to configure other Ethernet CFM service options:

```
    maximum-meps 4000
    log continuity-check errors
    commit
    exit
   exit
  exit
```

MEP Configuration: Example

This example shows how to configure a MEP for Ethernet CFM on an interface:

```
 RP/0/RP0:hostname# configure
 RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/1
 RP/0/RP0:hostname(config-if)# ethernet cfm
 RP/0/RP0:hostname(config-if-cfm)# mep domain Dm1 service Sv1 mep-id 1
 RP/0/RP0:hostname(config-if-cfm-mep)# commit
```

Ethernet CFM Show Command: Examples

These examples show how to verify the configuration of Ethernet Connectivity Fault Management (CFM):

Example 1

This example shows how to display all the maintenance points that have been created on an interface:

```
RP/0/RP0:hostname# show ethernet cfm local maintenance-points

Domain/Level         Service             Interface                 Type      ID         MAC
-------------------- ------------------- -----------------        ----   --------    -------
fig/5                bay                 TenGigE0/10/0/12.23456   Dn MEP    2
44:55:66
fig/5                bay                 TenGigE0/0/1/0.1         MIP
55:66:77
fred/3               barney              TenGigE0/1/0/0.1         Up MEP    5
66:77:88!
```

Example 2

This 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
* MIP creation configured using bridge-domain blort, but bridge-domain blort does not exist.

 * An Up MEP is configured for this domain on interface TenGigE0/1/2/3.234 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
```

Example 3

This example shows how to display operational state for local maintenance end points (MEPs):

```
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 TenGigE1/1/0/1.234 (Up)  Up     0/0   N  A       L7

Domain fred (level 5), Service barney
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
    2 TenGigE0/1/0/0.234 (Up)  Up     3/2   Y  RPC     L6
Domain foo (level 6), Service bar
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
  100 TenGigE1/1/0/1.234 (Up)  Up     0/0   N  A

Domain fred (level 5), Service barney
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
    2 TenGigE0/1/0/0.234 (Up)  Up     3/2   Y  RPC
```

Example 4

This example shows how to display operational state of other maintenance end points (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)
```

```
Domain fred (level 7), Service barney
Up MEP on TenGigE0/1/0/0.234, MEP-ID 2
================================================================================
St    ID MAC address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
 >     1 0011.2233.4455 Up      00:00:01         1234      0     0     0
R>     4 4455.6677.8899 Up      1d 03:04         3456      0   234     0
L      2 1122.3344.5566 Up      3w 1d 6h         3254      0     0  3254
C      2 7788.9900.1122 Test    00:13            2345      6    20  2345
X      3 2233.4455.6677 Up      00:23              30      0     0    30
I      3 3344.5566.7788 Down    00:34           12345      0   300  1234
V      3 8899.0011.2233 Blocked 00:35              45      0     0    45
 T     5 5566.7788.9900         00:56              20      0     0     0
M      6                                            0      0     0     0
U>     7 6677.8899.0011 Up      00:02             456      0     0     0

Domain fred (level 7), Service fig
Down MEP on TenGigE0/10/0/12.123, MEP-ID 3
================================================================================
St    ID MAC address    Port    Up/Downtime  CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- -------- ------ ----- -----
 >     1 9900.1122.3344 Up      03:45           4321      0     0     0
```

Example 5

This example shows how to display operational state of other maintenance end points (MEPs) detected by a local MEP with details:

```
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 00:00:06 ago:
     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
   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 00:00:04 ago:
     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
```

AIS for CFM Configuration: Examples

Example 1

This 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 D1 level 1
RP/0/RP0:hostname(config-cfm-dmn)# service Cross_Connect_1 xconnect group XG1 p2p
RP/0/RP0:hostname(config-cfm-dmn-svc)# ais transmission interval 1m cos 7
```

Example 2

This 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 Cross_Connect_1 xconnect group XG1 p2p
RP/0/RP0:hostname(config-cfm-dmn-svc)# log ais
```

This example shows how to configure AIS transmission on a CFM interface.

```
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface TenGigE 0/1/0/2
RP/0/RP0:hostname(config-if)# ethernet cfm
RP/0/RP0:hostname(config-if-cfm)# ais transmission up interval 1m cos 7
```

AIS for CFM Show Commands: Examples

This section includes the following examples:

show ethernet cfm interfaces ais Command: Example

This 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
------------------------ ---  - -------  -------  - --- ------------ --------
TenGi0/1/0/0.234 (Up)    Dn   5 RPC      6        7 1s  01:32:56 ago     5576
TenGi0/1/0/0.567 (Up)    Up   0 M        2,3      5 1s  00:16:23 ago      983
TenGi0/1/0/1.1 (Dn)      Up     D                 7 60s 01:02:44 ago     3764
TenGi0/1/0/2 (Up)        Dn   0 RX       1!
```

show ethernet cfm local meps Command: Examples

Example 1: Default

The following example shows how to display statistics for local maintenance end points (MEPs):

```
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 TenGigE1/1/0/1.234 (Up)  Up      0/0   N  A       7

Domain fred (level 5), Service barney
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ------------------------ --- -------- -- ------- ---
    2 TenGigE0/1/0/0.234 (Up)  Up      3/2   Y  RPC     6
```

Example 2: Domain Service

The following example shows how to display statistics for MEPs in a domain service:

```
RP/0/RP0:hostname# show ethernet cfm local meps domain foo service bar 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
```

Example 3: Verbose

The following example shows how to display verbose statistics for MEPs in a domain service:

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 any thing other than zero, since CCMs are only discarded when the limit on the number of peer MEPs is reached.

```
RP/0/RP0:hostname# show ethernet cfm local meps domain foo service bar 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)

  Packet        Sent      Received
  ------  ----------  -----------------------------------------------------
  CCM              20            20  (out of seq: 0)
  AIS            5576            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 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

  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
  LCK              -             0
```

Example 4: Detail

The following example shows how to display detailed statistics for MEPs in a domain service:

```
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
```

CFM - Sample Configuration Workflow

Complete these configurations on the provider edge routers to enable Connectivity Fault Management (CFM).

Topology

```
----(Te0/3/0/11)NCS4K-PE1(Hu0/5/0/0)-----(Hu0/5/0/0)NCS4K-PE2(Te0/5/0/9)----
```

where:

- TenGigE0/3/0/11 and TenGigE0/5/0/9 are the access or customer interfaces
- The HundredGigE0/5/0/0 interfaces are the core interfaces.
- PE1 and PE2 are the two L2VPN provider edge (PE) routers. The two PEs are typically connected at two different sites with an MPLS core between them. The attachment circuits (ACs)connected at each L2VPN PE are linked by a pseudowire (PW) over the MPLS network.

Task 1: Bring up the controllers in lan phy or packet termination mode.

Sample Configuration on PE1	Sample Configuration on PE2

`!`
`controller Optics0/3/0/11`
`port-mode Ethernet framing packet rate 10GE`
`no shut`
`!`
`controller Optics0/5/0/0`
`port-mode Ethernet framing packet rate 100GE`
`no shut`
`!`
	`!`
	`controller Optics0/5/0/9`
	`port-mode Ethernet framing packet rate 10GE`
	`no shut`
	`!`
	`controller Optics0/5/0/0`
	`port-mode Ethernet framing packet rate 100GE`
	`no shut`
	`!`

Task 2: Bring up the access and core interfaces.

Sample Configuration on PE1	Sample Configuration on PE2

Access interface:
`interface TenGigE0/3/0/11`
`!`
`interface TenGigE0/3/0/11.1 l2transport`
`encapsulation dot1q 1`
`no shut`
`!`
`interface TenGigE0/3/0/11.2 l2transport`
`encapsulation dot1q 2`
`no shut`
`!`
Core interface:
`interface HundredGigE0/5/0/0`
`ipv4 address 1.76.1.1 255.255.255.0`
` !`
`!`
	Access interface:
	`interface TenGigE0/5/0/9`
	`!`
	`interface TenGigE0/5/0/9.1 l2transport`
	`encapsulation dot1q 1`
	`no shut`
	`!`
	`interface TenGigE0/5/0/9.2 l2transport`
	`encapsulation dot1q 2`
	`no shut`
	`!`
	Core interface:
	`interface HundredGigE0/5/0/0`
	`ipv4 address 1.76.1.2 255.255.255.0`
	` !`
	`!`

Details: Two access interfaces are brought up so that two pseudowires can be created.	

Task 3: Define loopback address.

Sample Configuration on PE1	Sample Configuration on PE2
! interface Loopback0 ipv4 address 1.1.1.1 255.255.255.255 !	! interface Loopback0 ipv4 address 3.3.3.3 255.255.255.255 !

Task 4: Configure the routing process using OSPF or ISIS on the core interface.

Sample Configuration on PE1	Sample Configuration on PE2
router ospf 100 router-id 1.1.1.1 nsf nsr area 0 mpls traffic-eng interface Loopback0 ! interface HundredGigE0/5/0/0 ! ! mpls traffic-eng router-id Loopback0 !	router ospf 100 router-id 3.3.3.3 nsf nsr area 0 mpls traffic-eng interface Loopback0 ! interface HundredGigE0/5/0/0 ! ! mpls traffic-eng router-id Loopback0 !
Details: The sample configuration uses OSPF.	

Task 5: Configure MPLS traffic engineering on the core interface.

Sample Configuration on PE1	Sample Configuration on PE2
mpls traffic-eng interface HundredGigE0/5/0/0 ! fault-oam !	mpls traffic-eng interface HundredGigE0/5/0/0 ! fault-oam !

Task 6: Configure RSVP on the core interface.

Sample Configuration on PE1	Sample Configuration on PE2
rsvp interface HundredGigE0/5/0/0 bandwidth 100 ! !	rsvp interface HundredGigE0/5/0/0 bandwidth 100 ! !

Task 7: Configure MPLS OAM for MPLS pseudowires to work on the core interfaces.

Sample Configuration on PE1	Sample Configuration on PE2
! mpls oam !	! mpls oam !

Task 8: Configure the tunnel interface. It can be a MPLS-TE or Flex-LSP tunnel.

Sample Configuration on PE1	Sample Configuration on PE2

Sample Configuration on PE1	Sample Configuration on PE2
MPLS TE tunnel:	MPLS TE tunnel:
`interface tunnel-te1`	`interface tunnel-te1`
`ipv4 unnumbered Loopback0`	`ipv4 unnumbered Loopback0`
`signalled-bandwidth 1`	`signalled-bandwidth 1`
`destination 3.3.3.3`	`destination 1.1.1.1`
`path-selection`	`path-selection`
`metric te`	`metric te`
`bandwidth 50000`	`bandwidth 50000`
`!`	`!`
` path-option 1 dynamic`	` path-option 1 dynamic`
`!`	`!`
Flex-LSP tunnel with BFD:	Flex-LSP tunnel with BFD:
`interface tunnel-te2`	`interface tunnel-te2`
`ipv4 unnumbered Loopback0`	`ipv4 unnumbered Loopback0`
`bfd`	`bfd`
` encap-mode gal`	` encap-mode gal`
` multiplier 3`	` multiplier 3`
` fast-detect`	` fast-detect`
` minimum-interval 100`	` minimum-interval 100`
` !`	` !`
` signalled-bandwidth 1`	` signalled-bandwidth 1`
` destination 3.3.3.3`	` destination 1.1.1.1`
` bidirectional`	` bidirectional`
` association id 86 source-address 192.0.0.0`	` association id 86 source-address 192.0.0.0`
` association type co-routed`	` association type co-routed`
`   fault-oam`	`   fault-oam`
`  !`	`  !`
` !`	` !`
`path-selection`	`path-selection`
`  metric te`	`  metric te`

Sample Configuration on PE1	Sample Configuration on PE2
bandwidth 50000 ! path-option 1 dynamic !	bandwidth 50000 ! path-option 1 dynamic !

Task 9: Setup interfaces running LDP:

Sample Configuration on PE1	Sample Configuration on PE2
mpls ldp nsr log neighbor nsr graceful-restart ! graceful-restart reconnect-timeout 169 graceful-restart forwarding-state-holdtime 180 discovery targeted-hello holdtime 180 targeted-hello interval 20 ! router-id 1.1.1.1 session protection address-family ipv4 discovery targeted-hello accept ! !	mpls ldp nsr log neighbor nsr graceful-restart ! graceful-restart reconnect-timeout 169 graceful-restart forwarding-state-holdtime 180 discovery targeted-hello holdtime 180 targeted-hello interval 20 ! router-id 3.3.3.3 session protection address-family ipv4 discovery targeted-hello accept ! !
Details: The two PEs establish a targeted MPLS LDP session between themselves so they can establish and control the status of the pseudowire. The targeted MPLS LDP session is established over MPLS-TE or Flex LSP.	

Task 10: Configure VPWS static and dynamic pseudowires.

Sample Configuration on PE1	Sample Configuration on PE2

Pseudowire 1 (vpws-pw-1) uses MPLS-TE tunnel (tunnel-te 1):
`l2vpn`
`pw-class vpws-pw-1`
`encapsulation mpls`
`protocol ldp`
`ipv4 source 1.1.1.1`
`preferred-path interface tunnel-te 1`
` !`
	Pseudowire 1 (vpws-pw-1) uses MPLS-TE tunnel (tunnel-te 1):
	`l2vpn`
	`pw-class vpws-pw-1`
	`encapsulation mpls`
	`protocol ldp`
	`ipv4 source 3.3.3.3`
	`preferred-path interface tunnel-te 1`
	` !`

Pseudowire 2 (vpws-pw-2) uses Flex-LSP tunnel (tunnel-te 2):
`!`
` pw-class vpws-pw-2`
` encapsulation mpls`
` protocol ldp`
` ipv4 source 1.1.1.1`
` preferred-path interface tunnel-te 2`
`!`
	Pseudowire 2 (vpws-pw-2) uses Flex-LSP tunnel (tunnel-te 2):
	`!`
	` pw-class vpws-pw-2`
	` encapsulation mpls`
	` protocol ldp`
	` ipv4 source 3.3.3.3`
	` preferred-path interface tunnel-te 2`
	`!`

Configure pseudowire 1 (vpws-pw-1) as dynamic:
`!`
` xconnect group vpws`
` p2p pw1`
` interface TenGigE0/3/0/11.1`
` neighbor ipv4 3.3.3.3 pw-id 1`
` bandwidth 1000`
` pw-class vpws-pw-1`
` !`
	Configure pseudowire 1 (vpws-pw-1) as dynamic:
	`!`
	` xconnect group vpws`
	` p2p pw1`
	` interface TenGigE0/5/0/9.1`
	` neighbor ipv4 1.1.1.1 pw-id 1`
	` bandwidth 1000`
	` pw-class vpws-pw-1`
	` !`

Sample Configuration on PE1	Sample Configuration on PE2

Configure pseudowire 2(vpws-pw-2) as static:
`!`
`p2p pw2`
`interface TenGigE0/3/0/11.2`
`neighbor ipv4 3.3.3.3 pw-id 2`
`mpls static label local 100 remote 200`
`bandwidth 1000`
`pw-class vpws-pw-2`
`   !`
`!`
	Configure pseudowire 2(vpws-pw-2) as static:
	`!`
	`p2p pw2`
	`interface TenGigE0/5/0/9.2`
	`neighbor ipv4 1.1.1.1 pw-id 2`
	`mpls static label local 100 remote 200`
	`bandwidth 1000`
	`pw-class vpws-pw-2`
	`   !`
	`!`

Task 11: Configure Connectivity Fault Management (CFM).

Sample Configuration on PE1	Sample Configuration on PE2

	`l2vpn`
	`xconnect group xc1`
	`p2p pw2`
	`interface TenGigE0/5/0/9`
	`interface HundredGigE0/5/0/0`
	`!`
	`!`

`domain MD2 level 2 id null`
`service up_mep_customer_1 xconnect group xc1 p2p p1 id number 1`
`continuity-check interval 100ms`
`mep crosscheck`
`mep-id 4001 mac-address 7ef2.fe69.312b`
`!`
	`domain MD2 level 2 id null`
	`service up_mep_customer_1 xconnect group xc1 p2p p1 id number 1`
	`continuity-check interval 100ms`
	`mep crosscheck`
	`mep-id 1 mac-address 78ba.f99b.b9ea`
	`!`

Sample Configuration on PE1	Sample Configuration on PE2
ais transmission interval 1s cos 0 log ais log continuity-check errors log crosscheck errors log continuity-check mep changes ! !	ais transmission interval 1s cos 0 log ais log continuity-check errors log crosscheck errors log continuity-check mep changes ! !
	interface TenGigE0/5/0/9 l2transport encapsulation dot1q 1 ethernet cfm mep domain MD2 service up_mep_customer_1 mep-id 4001 ! ! !
interface TenGigE0/3/0/11 l2transport encapsulation dot1q 1 ethernet cfm mep domain MD2 service up_mep_customer_1 mep-id 1 ! ! !	interface HundredGigE0/5/0/0 l2transport encapsulation dot1q 1 ethernet cfm mep domain MD1 service down_mep_customer_10001 mep-id 4001 ! ! !

EFD Configuration: 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 id null
```

```
RP/0/RP0:hostname(config-cfm-dmn)# service S1 down-meps id number 1
RP/0/RP0:hostname(config-cfm-dmn-svc)# efd
```

This 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 id null
RP/0/RP0:hostname(config-cfm-dmn)# service S1 down-meps id number 1
RP/0/RP0:hostname(config-cfm-dmn-svc)# log efd
```

Displaying EFD Information: Examples

The following examples show how to display information about EFD:

show efd interfaces Command: Example

This example shows how to display all interfaces that are shut down in response to an EFD action:

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

Server VLAN MA
==============
Interface         Clients
-------------------------
TenGigE0/0/0/0.0     CFM
```

show ethernet cfm local meps detail Command: Example

Use the **show ethernet cfm local meps detail** command to display MEP-related EFD status information. The following example shows that EFD is triggered for MEP-ID 100:

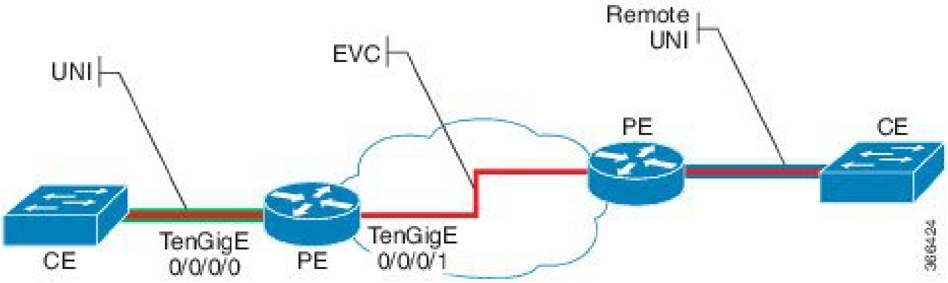
```
RP/0/RP0:hostname# show ethernet cfm local meps detail

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)
  Cross-check errors: 2 missing, 0 unexpected

  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:           Yes

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, 0 with errors, 0 timed out (archived)
  Cross-check errors: 0 missing, 0 unexpected

  CCM generation enabled:  Yes (Remote Defect detected: No)
  AIS generation enabled:  Yes (level: 6, interval: 1s)
  Sending AIS:             No
  Receiving AIS:           No
  EFD triggered:           No
```

Note You can also verify that EFD has been triggered on an interface using the **show interfaces** and **show interfaces brief** commands. When an EFD trigger has occurred, these commands will show the interface status as *up* and the line protocol state as *down*.

Configuration Example for Ethernet LMI

Figure below shows a basic E-LMI network environment with a local UNI defined as the PE using Ten-Gigabit Ethernet interface 0/0/0/0, and connectivity to a remote UNI over Ten-Gigabit Ethernet interface 0/0/0/1.

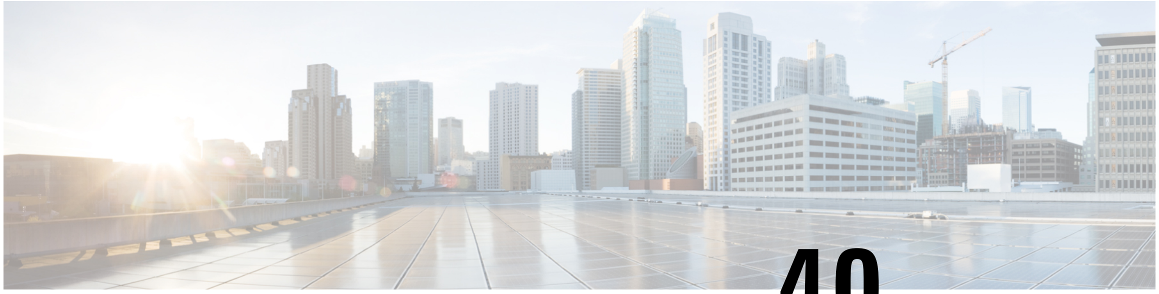
Figure 30: Basic E-LMI UNI and Remote UNI Diagram



The following configuration provides a basic E-LMI configuration for the environment shown in figure above, as the PE device on the local UNI with physical Ten-Gigabit Ethernet interfaces 0/0/0/0 and 0/0/0/1:

```
RP/0/RP0:hostname# configure
!
! Configure the Local UNI EFPs
!
RP/0/RP0:hostname(config)# interface TenGigE0/0/0/0.0 l2transport
RP/0/RP0:hostname(config-subif)#encapsulation dot1q 1-20
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface TenGigE0/0/0/1.1 l2transport
RP/0/RP0:hostname(config-subif)# #encapsulation dot1q 1-20
RP/0/RP0:hostname(config-subif)# exit
!
! Create the EVC
!
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# bridge group BG1
RP/0/RP0:hostname(config-l2vpn-bg)# bridge-domain BD1
RP/0/RP0:hostname(config-l2vpn-bg-bd)# interface TenGigE0/0/0/0.0
RP/0/RP0:hostname(config-l2vpn-bg-bd)# interface TenGigE0/0/0/1.1
RP/0/RP0:hostname(config-l2vpn-bg-bd)# exit
RP/0/RP0:hostname(config-l2vpn-bg)# exit
RP/0/RP0:hostname(config-l2vpn)# exit
!
! Configure Ethernet CFM
!
RP/0/RP0:hostname(config)# ethernet cfm
RP/0/RP0:hostname(config-cfm)# domain GLOBAL level 5
RP/0/RP0:hostname(config-cfm-dmn)# service CustomerA bridge group BG1 bridge-domain BD1
RP/0/RP0:hostname(config-cfm-dmn-svc)# continuity-check interval 100ms
RP/0/RP0:hostname(config-cfm-dmn-svc)# mep crosscheck mep-id 22
RP/0/RP0:hostname(config-cfm-dmn-svc)# mep crosscheck mep-id 11
RP/0/RP0:hostname(config-cfm-dmn-svc)# exit
```

```
RP/0/RP0:hostname(config-cfm-dmn)# exit
RP/0/RP0:hostname(config-cfm)# exit
!
! Configure EFPs as CFM MEPs
!
RP/0/RP0:hostname(config)# interface TenGigE0/0/0/0.0 l2transport
RP/0/RP0:hostname(config-subif)# ethernet cfm
RP/0/RP0:hostname(config-if-cfm)# mep domain GLOBAL service CustomerA mep-id 22
RP/0/RP0:hostname(config-if-cfm)# exit
RP/0/RP0:hostname(config-subif)# exit
!
! Configure the Local UNI Name
!
RP/0/RP0:hostname(config)# interface TenGigE 0/0/0/0
RP/0/RP0:hostname(config-if)# ethernet uni id PE1-CustA-Slot0-Port0
RP/0/RP0:hostname(config-if)# exit
!
! Enable E-LMI on the Local UNI Physical Interface
!
RP/0/RP0:hostname(config)# interface TenGigE 0/0/0/0
RP/0/RP0:hostname(config-if)# ethernet lmi
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# commit
```



CHAPTER 40

Configure Ethernet Service Activation Test

This chapter describes the Cisco IOS XR commands to configure Y.1564 - Ethernet Service Activation Test (SAT).

Understanding Y.1564 - Ethernet Service Activation Test

Table 39: Feature History

Feature Name	Release Information	Feature Description
Y.1564 - Ethernet Service Activation Test (SAT)	Cisco IOS XR Release 6.5.31	Y.1564 – Ethernet SAT is a standards-based test methodology to test turn up, installation, and troubleshooting of Ethernet-based services. This test methodology allows you to measure Frame Transfer Delay (FTD) or latency and Frame Loss Ratio (FLR) parameters. Commands added: • ethernet service-activation-test • profile • outer-cos • duration • color-aware • information-rate • packet-size • show ethernet service-activation-test

Table 40: Feature History

Feature Name	Release Information	Feature Description
Y.1564 Ethernet SAT Support on Multi-chassis	Cisco IOS XR Release 6.5.32	Y.1564 – Ethernet SAT feature supports up to four parallel SAT sessions in single chassis and up to four parallel SAT sessions for each rack in multi-chassis.

Ethernet services have evolved significantly with the deployment of Ethernet in service provider networks. Ethernet is not only found at the User Network Interface (UNI) but can also be deployed anywhere in the network, creating a Network-to-Network Interface (NNI). With the capability to prioritize traffic, high availability, and its built-in resiliency, service providers are now using Ethernet technology to deliver advanced services. In the absence of any standardized test methodologies that can measure delay and loss, the ITU-T Y.1564 recommendation addresses this gap.

Y.1564 - Ethernet Service Activation Test (SAT) is a testing procedure which tests service turn-up, installation, and troubleshooting of Ethernet-based services. This test methodology was created to have a standard way of measuring Ethernet-based services in the industry.

Cisco's implementation of ITU-T Y.1564 has three key objectives:

- Serve as a network service level agreement (SLA) validation tool, ensuring that a service meets its guaranteed performance settings in a controlled test time.
- Ensure that all the services carried by the network meet their SLA objectives at their maximum committed rate.
- Perform medium-term and long-term service testing, confirming that network element can properly carry all the services while under stress during a soaking period.

The following Key Performance Indicators (KPI) metrics are collected to ensure that the configured SLAs are met for the service or stream.

- Frame Transfer Delay (FTD) or latency—Measures the round-trip time (RTT) taken by a test frame to travel through a network device, or across the network and back to the test port.
- Frame Loss Ratio (FLR)—Measures the number of packets lost from the total number of packets sent. Frame loss can be due to a number of issues such as network congestion or errors during transmissions.

Note

- Rewrite with POP option is supported with Color Blind mode with Outer-Cos value of 0.
- Rewrite with POP option is not supported when the second VLAN tag is "any".

Note The maximum number of parallel SAT sessions supported is four in single chassis and four for each rack in multi-chassis.

Note If the bundle interface has members on rack 1 and rack 2, the number of parallel SAT sessions supported is two in rack 1 and two in rack 2.

Supported Modes

The mode of operation that is supported for Y.1564 is the two-way statistics collection mode. In the two-way mode, the sender generates the test traffic used to perform the test, which is then looped back by the remote node. The statistics are measured and collected locally on the sender.

The following encapsulations are supported by Y.1564 SAT feature:

- dot1q
- dot1q + second dot1q
- dot1ad
- dot1ad + second dot1q

- priority tagged
- untagged

Supported Bandwidth Parameters

Bandwidth Parameters	Internal Direction	External Direction
Commited Information Rate	Y	Y
Exceeded Information Rate	Y	Y

SAT Target Matrix

Target	Internal Direction	External Direction
L2 Interface over physical main or sub interfaces	Y	Y
L2 Interface over bundle main or sub interfaces	Y	Y
L2 PW VPWS over physical main or sub interfaces	Y	Y
L2 PW VPWS over bundle main or sub interfaces	Y	Y
XConnect over physical main or sub interfaces	Y	Y
XConnect over bundle main or sub interfaces	Y	Y

Configuring Color Profile for Ethernet SAT

The following example shows how to configure a color-blind profile for Ethernet SAT.

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#ethernet service-activation-test
RP/0/RP0:hostname(config-ethsat)#profile sattest1
RP/0/RP0:hostname(config-ethsat-prf)#outer-cos 4
RP/0/RP0:hostname(config-ethsat-prf)#duration 8 minutes
RP/0/RP0:hostname(config-ethsat-prf)#information-rate 11800 mbps
RP/0/RP0:hostname(config-ethsat-prf)#packet-size 1000
```

The following example shows how to configure a color-aware profile for Ethernet SAT.

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#ethernet service-activation-test
RP/0/RP0:hostname(config-ethsat)#profile sattest3
RP/0/RP0:hostname(config-ethsat-prf)#outer-cos 4
RP/0/RP0:hostname(config-ethsat-prf)#duration 1 minutes
RP/0/RP0:hostname(config-ethsat-prf)#color-aware cir 7 gbps eir-color cos 1
RP/0/RP0:hostname(config-ethsat-prf)#information-rate 8 gbps
RP/0/RP0:hostname(config-ethsat-prf)#packet-size 1000
```

Configuration Examples

The following example shows how to start service-activation test on an interface with external direction.

```
RP/0/RP0:hostname#ethernet service-activation-test start interface TenGigE 10/0/0/1 profile
 test destination 00ab.6009.9c3c direction external
```

The following example shows how to start service-activation test on an interface with internal direction.

```
RP/0/RP0:hostname#ethernet service-activation-test start interface TenGigE 10/0/0/1 profile
 test destination 00ab.6009.9c3c direction internal
```

The following example shows how to stop service-activation-test on an interface.

```
RP/0/RP0:hostname#ethernet service-activation-test stop interface TenGigE 10/0/0/1
```

The following example shows how to stop all service-activation-tests.

```
RP/0/RP0:hostname#ethernet service-activation-test stop all
```

Verification

To verify the interfaces on which Y.1564 is enabled, use the **show ethernet service-activation-test brief** command. The following is a sample output of an enabled device.

```
RP/0/RP0:hostname#show ethernet service-activation-test brief
Interface                  Permissions          Test Status
---------------------------------------------------------------------------
Bundle-Ether10.1           Internal only      In progress, 1 min(s) left
Te0/0/0/9.2                External only           None started
Te0/0/0/9.2                Internal only           Completed
```

CHAPTER 41

Ethernet Local Management Interface

This chapter provides conceptual and configuration information of the Ethernet Local Management Interface protocol.

Ethernet Local Management Interface

Ethernet Local Management Interface (E-LMI) is an asymmetric protocol that runs on the Provider Edge (PE) to Customer Edge (CE) link. The user-facing Provider Edge (uPE) device uses E-LMI to communicate status and configuration parameters of Ethernet Virtual Circuits (EVCs) available on the User-Network Interface (UNI) to the CE device. E-LMI defines the message formats and procedures for conveying the information from uPE to CE, however it does not define the method by which the information is collected on the PE.

The basic operation of E-LMI involves the uPE device providing connectivity status and configuration parameters to the CE using the STATUS messages in response to STATUS ENQUIRY messages set by the CE to the uPE.

E-LMI Communication

This section discusses the E-LMI messaging and system parameter details.

Messaging

The E-LMI protocol as defined by the MEF 16 standard, defines the use of only two message types—STATUS ENQUIRY and STATUS.

These E-LMI messages consist of required and optional fields called information elements, and all information elements are associated with assigned identifiers. All messages contain the Protocol Version, Message Type, and Report Type information elements, followed by optional information elements and sub-information elements.

E-LMI messages are encapsulated in 46- to 1500-byte Ethernet frames, which are based on the IEEE 802.3 untagged MAC-frame format. E-LMI frames consist of the following fields:

- Destination address (6 bytes)—Uses a standard MAC address of 01:80:C2:00:00:07.
- Source address (6 bytes)—MAC address of the sending device or port.
- E-LMI Ethertype (2 bytes)—Uses 88-EE.
- E-LMI PDU (46–1500 bytes)—Data plus 0x00 padding as needed to fulfill minimum 46-byte length.
- CRC (4 bytes)—Cyclic Redundancy Check for error detection.

For more details about E-LMI messages and their supported information elements, refer to the *Metro Ethernet Forum, Technical Specification MEF 16, Ethernet Local Management Interface (E-LMI), January 2006*.

Parameters

For correct interaction between the CE and the PE, each device has two configurable parameters. The CE uses a Polling Timer (PT) and a Polling Counter; the PE uses a Polling Verification Timer (PVT) and a Status Counter.

Cisco Proprietary Remote UNI Details Information Element

The E-LMI MEF 16 specification does not define a way to send proprietary information.

To provide additional information within the E-LMI protocol, the Cisco IOS XR software implements a Cisco-proprietary information element called Remote UNI Details to send information to the CE about remote UNI names and states. This information element implements what is currently an unused identifier from the E-LMI MEF 16 specification.

E-LMI Operation

The basic operation of E-LMI consists of a CE device sending periodic STATUS ENQUIRY messages to the PE device, followed by mandatory STATUS message responses by the PE device that contain the requested information. Sequence numbers are used to correlate STATUS ENQUIRY and STATUS messages between the CE and PE.

The CE sends the following two forms of STATUS ENQUIRY messages called Report Types:

- E-LMI Check—Verifies a Data Instance (DI) number with the PE to confirm that the CE has the latest E-LMI information.
- Full Status—Requests information from the PE about the UNI and all EVCs.

The CE device uses a polling timer to track sending of STATUS ENQUIRY messages, while the PE device can optionally use a Polling Verification Timer (PVT), which specifies the allowable time between transmission of the PE's STATUS message and receipt of a STATUS ENQUIRY from the CE device before recording an error.

In addition to the periodic STATUS ENQUIRY/STATUS message sequence for the exchange of E-LMI information, the PE device also can send asynchronous STATUS messages to the CE device to communicate changes in EVC status as soon as they occur and without any prompt by the CE device to send that information.

Both the CE and PE devices use a status counter (N393) to determine the local operational status of E-LMI by tracking consecutive errors received before declaring a change in E-LMI protocol status.

Supported Functions

The Cisco NCS 4000 Series Router serves as the PE device for E-LMI, and supports the following PE functions:

- Supports the E-LMI protocol on Ethernet physical interfaces that are configured with Layer 2 subinterfaces as Ethernet Flow Points (EFPs), which serve as the EVCs about which the physical interface reports status to the CE. The Cisco IOS XR software does not support a specific manageability context for an Ethernet Virtual Connection (EVC).
- Provides the ability to configure the following E-LMI options defined in the MEF 16 specification:
  - T392 Polling Verification Timer (PVT)
  - N393 Status Counter
- Sends notification of the addition and deletion of an EVC.
- Sends notification of the availability (active) or unavailability (inactive, partially active) status of a configured EVC.
- Sends notification of the local UNI name.
- Sends notification of remote UNI names and states using the Cisco-proprietary Remote UNI Details information element, and the ability to disable the Cisco-proprietary Remote UNI information element.
- Sends information about UNI and EVC attributes to the CE (to allow the CE to auto-configure these attributes), including:
  - CE-VLAN to EVC Map
  - CE-VLAN Map Type (Bundling, All-to-one Bundling, Service Multiplexing)
  - Service Type (point-to-point or multipoint)
- Uses CFM Up MEPs to retrieve the EVC state, EVC Service Type, and remote UNI details.
- Provides the ability to retrieve the per-interface operational state of the protocol (including all the information currently being communicated by the protocol to the CE) using the command-line interface (CLI) or Extensible Markup Language (XML) interface.
- Supports one E-LMI session per physical interface; maximum of 80 per linecard.
- Supports up to 4000 EVCs total per linecard for all physical interfaces enabled for E-LMI.

Limitations

This sections lists the implementation limitations of the E-LMI protocol. The following are not supported:

- CE-specific features are not supported.
- Retrieval of the EVC status from MPLS OAM.
- Communication of UNI and EVC bandwidth profiles to the CE.
- Operation of the protocol during linecard MDR events.

Enable ELMI and configure the parameters

Before enabling E-LMI on a Cisco NCS 4000 router, complete the following tasks:

1. Create EVCs by configuring EFPs
2. Configure xconnect groups
3. Configure CFM
4. Configure UNI IDs

All of these tasks, have been discussed in the later sections.

E-LMI is configured per interface. It can be configured only on physical ethernet interfaces using CLI commands (or XML schema). The configuration items and their possible values are described in the following table:

Parameter	Description	Allowed value(s)	Default value
Status Counter	Threshold to the number of consecutive events before an operational state change is made.	2 to 10	4
Polling Verification Timer	Determines the interval for which the PE will wait for a status enquiry before reporting an error.	5 to 30 seconds; disabled	15 seconds
Remote UNI Extension	Disables transmission of Cisco-proprietary Remote UNI Details, to provide stricter conformance with the MEF standard.	disabled/ enabled	enabled
Log errors	Disables the syslog messages emitted when a protocol or reliability error is detected.	disabled/ enabled	enabled

Parameter	Description	Allowed value(s)	Default value
Log events	Disables the syslog messages emitted when a change to the operational status of the E-LMI protocol occurs.	disabled/ enabled	enabled

Prerequisites for Configuring E-LMI

Before you begin with the required tasks, be sure to complete the following requirements:

- Identify the local and remote UNIs in your network where you want to run E-LMI, and define a naming convention for them.
- Enable E-LMI on the corresponding CE interface link on a device that supports E-LMI CE operation.

Create EVC

EVCs for E-LMI are established by first configuring EFPs (Layer 2 subinterfaces) on the local UNI physical Ethernet interface link to the CE where E-LMI will be running, and also on the remote UNI link. Then, the EFPs need to be assigned to an xconnect domain to create the EVC.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostnamerouter# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE**] *interface-path-id***.***subinterface* **l2transport**

Example:

```
RP/0/RP0:hostname:router(config)# interface tengige 0/0/0/0.0 l2transport
```

Creates a VLAN subinterface in Layer 2 transport mode and enters Layer 2 subinterface configuration mode.

Step 3 **encapsulation dot1q** *vlan-id* [**, untagged** | **,** *vlan-id* | –*vlan-id*] [**exact** | **ingress source-mac** *mac-address* | **second-dot1q** *vlan-id*]

Example:

```
RP/0/RP0:hostname:router(config-subif)# encapsulation dot1q 1-20
```

Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

Step 4 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-subif)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

  ```
  Uncommitted changes found, commit them before exiting(yes/no/cancel)?
  [cancel]:
  ```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

What to do next

Configure a xconnect group

Configure cross-connect (xconnect) groups

To configure a cross-connect group and assign EFPs, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **l2vpn**

Example:

```
RP/0/RP0:hostname:router(config)# l2vpn
```

Enters L2VPN configuration mode.

Step 3 **xconnect group** *xconnect-group-name*

Example:

```
RP/0/RP0:hostname:router(config-l2vpn)# xconnect group g1
```

Enters the cross-connect (xconnect) group configuration mode.

Step 4 **interface** [**TenGigE**] *interface-path-id***.***subinterface*

Example:

```
RP/0/RP0:hostname:router(config-l2vpn-xconnect)# interface TenGigE0/13/0/6.2
```

Associates the EFP (EVC) with the specified cross-connect group, where *interface-path-id* is specified as the *rack*/*slot*/*module*/*port* location of the interface and ***.****subinterface* is the subinterface number.

Repeat this step for as many EFPs (EVCs) as you want to associate with the cross-connect group.

Step 5 **interface** [**TenGigE**] *interface-path-id***.***subinterface*

Example:

```
RP/0/RP0:hostname:router(config-l2vpn-xconnect)# interface TenGigE0/13/0/7.2
```

Associates the EFP (EVC) with the specified cross-connect group , where *interface-path-id* is specified as the *rack*/*slot*/*module*/*port* location of the interface and ***.****subinterface* is the subinterface number.

The cross-connect is between the two configured interfaces.

Step 6 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-l2vpn-xconnect)# end
```

or

```
RP/0/RP0:hostname:router(config-l2vpn-)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

  ```
  Uncommitted changes found, commit them before exiting(yes/no/cancel)?
  [cancel]:
  ```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 7 **show l2vpn xconnect**

Example:

```
RP/0/RP0:hostname:router # show l2vpn xconnect
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
```

```
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                   Segment 1                       Segment 2
Group      Name       ST   Description           ST       Description           ST
------------------------   -----------------------------   -----------------------------
xconn_local
           xc3        UP   Te0/13/0/6.2          UP       Te0/13/0/7.2          UP
----------------------------------------------------------------------------------------
```

Verifies the xconnect configuration.

For more configurations with xconnect groups, see Layer 2 Local Switching, on page 623.

What to do next

Configure CFM

Configure Ethernet CFM

The Cisco NCS 4000 series router uses Ethernet CFM to monitor EVC status for E-LMI. To use CFM for E-LMI, a CFM maintenance domain and service must be configured on the router and the EFPs must be configured as CFM Maintenance End-points (MEP).

The minimum configuration to support E-LMI using Ethernet CFM is to configure a CFM maintenance domain and service on the router. Other CFM options can also be configured.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **interface tengige** *interface-path-id*.*subinterface* **l2transport**

Example:

```
RP/0/RP0:hostname:router(config)# interface tengige 0/0/0/0.0 l2transport
```

Enters Layer 2 subinterface configuration mode for the EFP.

Step 3 **ethernet cfm**

Example:

```
RP/0/RP0:hostname:router(config-subif)# ethernet cfm
```

Enters Ethernet CFM interface configuration mode.

Step 4 **mep domain** *domain-name* **service** *service-name* **mep-id** *id-number*

Example:

```
RP/0/RP0:hostname:router(config-if-cfm)# mep domain GLOBAL service CustomerA mep-id 22
```

Creates a MEP on an interface and enters interface CFM MEP configuration mode.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-if-cfm-mep)# commit
```

Saves configuration changes.

Step 6 **show ethernet cfm peer meps**

Example:

```
RP/0/RP0:hostname:router # 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    S - Standby

Domain local (level 3), Service custA
Up MEP on TenGigE0/13/0/6.2 MEP-ID 11
================================================================================
St    ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
>    22 78ba.f99b.a074 Up      00:02:17            0      0     0     0

Up MEP on TenGigE0/13/0/7.2 MEP-ID 22
================================================================================
St    ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
>    11 78ba.f99b.a073 Up      00:02:17            0      0     0     0
```

Verifies the CFM configuration.

For more CFM configurations, *see the CFM sections*.

What to do next

Provision UNI IDs

Configure UNI

It is recommended that you configure UNI names on the physical interface links to both the local and remote UNIs to aid in management for the E-LMI protocol. To configure UNI names, complete the following tasks on the physical interface links to both the local and remote UNIs:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **interface TenGigE** *interface-path-id*

Example:

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

Enters interface configuration mode for the physical interface.

Step 3 **ethernet uni id** *name*

Example:

```
RP/0/RP0:hostname:router(config-if)# ethernet uni id PE1-CustA-Slot0-Port0
```

Specifies a name (up to 64 characters) for the Ethernet UNI interface link.

Step 4 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-if)# commit
```

Saves configuration changes.

What to do next

Enable E-LMI

Enable E-LMI

E-LMI can be enabled only on physical ethernet interfaces.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname:router# interface tengige 0/0/0/0
```

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname:router(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# commit
```

Saves configuration changes.

What to do next

Verify the E-LMI configuration

Use the **show ethernet lmi interfaces detail** command to display the values for the Ethernet LMI configuration for a particular interface, or for all interfaces. The following example shows sample output for the command:

```
RP/0/RP0:hostname:router# show ethernet lmi interfaces detail
Interface: TenGigE0/13/0/6
  Ether LMI Link Status: Up
  UNI Id: PE1-CustA-slot13-Port6
  Line Protocol State: Up
  MTU: 1514 (1 PDU reqd. for full report)
  CE-VLAN/EVC Map Type: Service Multiplexing with no bundling (2 EVCs)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 139
  Last Sequence Numbers: Sent 18, Received 211
  Reliability Errors:
    Status Enq Timeouts                  0 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 Received  00:00:11 ago   Full Status Sent      00:00:11 ago
  PDU Received              00:00:01 ago   PDU Sent              00:00:01 ago
  LMI Link Status Changed   00:00:23 ago   Last Protocol Error      never
  Counters Cleared             never

  Sub-interface: TenGigE0/13/0/6.2
    VLANs: 1100
    EVC Status: Active
    EVC Type: Point-to-Point
    OAM Protocol: CFM
      CFM Domain: local (level 3)
      CFM Service: custA
    Remote UNI Count: Configured = 1, Active = 1
    Remote UNI Id                                                    Status
    -------------                                                    ------
    <Remote UNI Reference Id: 22>                                    Up
```

Configure Polling Verification Timer

The MEF T392 Polling Verification Timer (PVT) specifies the allowable time between transmission of a STATUS message and receipt of a STATUS ENQUIRY from the UNI-C before recording an error. The default value is 15 seconds.

To modify the default value or disable the PVT altogether, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname:router# interface tengige 0/0/0/0
```

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname:router(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **polling-verification-timer** {*interval* | **disable**}

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# polling-verification-timer 30
```

Sets or disables the MEF T392 Polling Verification Timer for E-LMI operation, which specifies the allowable time (in seconds) between transmission of a STATUS message and receipt of a STATUS ENQUIRY from the UNI-C before recording an error. The default is 15.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# commit
```

Saves configuration changes.

Configure Status Counter

The MEF N393 Status Counter value is used to determine E-LMI operational status by tracking receipt of consecutive good packets or successive expiration of the PVT on packets. The default counter is four, which means that while the E-LMI protocol is in Down state, four good packets must be received consecutively to change the protocol state to Up, or while the E-LMI protocol is in Up state, four consecutive PVT expirations must occur before the state of the E-LMI protocol is changed to Down on the interface.

To modify the status counter default value, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname:router# interface tengige 0/0/0/0
```

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname:router(config-if)# ethernet lmi
```

Enables Ethernet Local Management Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **status-counter** *threshold*

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# status-counter 5
```

Sets the MEF N393 Status Counter value that is used to determine E-LMI operational status by tracking receipt of consecutive good and bad packets from a peer. The default is 4.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# commit
```

Saves configuration changes.

Disable Syslog Messages

The E-LMI protocol tracks certain errors and events whose counts can be displayed using the **show ethernet lmi interfaces** command.

To disable syslog messages for E-LMI errors or events, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname:router# interface tengige 0/0/0/0
```

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname:router(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **log** {**errors** | **events**} **disable**

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# log events disable
```

Turns off syslog messages for E-LMI errors or events.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# commit
```

Saves configuration changes.

Disable Cisco-proprietary Remote UNI Details Information Element

To provide additional information within the E-LMI protocol, the Cisco IOS XR software implements a Cisco-proprietary information element called Remote UNI Details to send information to the CE about remote UNI names and states. This information element implements what is currently an unused identifier from the E-LMI MEF 16 specification.

To disable use of the Remote UNI Details information element, complete the following tasks:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname:router# configure
```

Enters global configuration mode.

Step 2 **interface** [**TenGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname:router# interface tengige 0/0/0/0
```

Enters interface configuration mode for the physical interface.

Step 3 **ethernet lmi**

Example:

```
RP/0/RP0:hostname:router(config-if)# ethernet lmi
```

Enables Ethernet Local Managment Interface operation on an interface and enters interface Ethernet LMI configuration mode.

Step 4 **extension remote-uni disable**

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# extension remote-uni disable
```

Disables transmission of the Cisco-proprietary Remote UNI Details information element in E-LMI STATUS messages.

Step 5 **end** or **commit**

Example:

```
RP/0/RP0:hostname:router(config-if-lmi)# commit
```

Troubleshooting E-LMI Configuration

This section describes some basic information for troubleshooting your E-LMI configuration in the following topics:

Link Status Troubleshooting

The E-LMI protocol operational status is reported in the “Ether LMI Link Status” or “ELMI state” fields in the output of forms of the **show ethernet lmi interfaces** command. To investigate a link status other than “Up,” consider the following guidelines:

- Unknown (PVT disabled)—Indicates that the Polling Verification Timer has been configured as disabled, so no status information can be provided. To see an “Up” or “Down” status, you must enable the PVT.
- Down—The E-LMI link status can be Down for the following reasons:
  - The PVT has timed out the number of times specified by the **status-counter** command. This indicates that STATUS ENQUIRY messages have not been received from the CE device. This can be for the following reasons:

    — The CE device is not connected to the PE device. Check that the CE device is connected to the interface on which E-LMI is enabled on the PE device.

    — The CE device is not sending Status Enquiries. Check that E-LMI is enabled on the CE interface which is connected to the PE device.

    — Protocol errors are causing the PVT to expire. The PVT is only reset when a valid (unerrored) STATUS ENQUIRY message is received.
  - The Line Protocol State is “Down” or “Admin Down.”
  - The protocol has not yet started on the interface because it does not have useful information to provide, such as the UNI Id or details about EVCs. This is a symptom of provisioning misconfiguration.

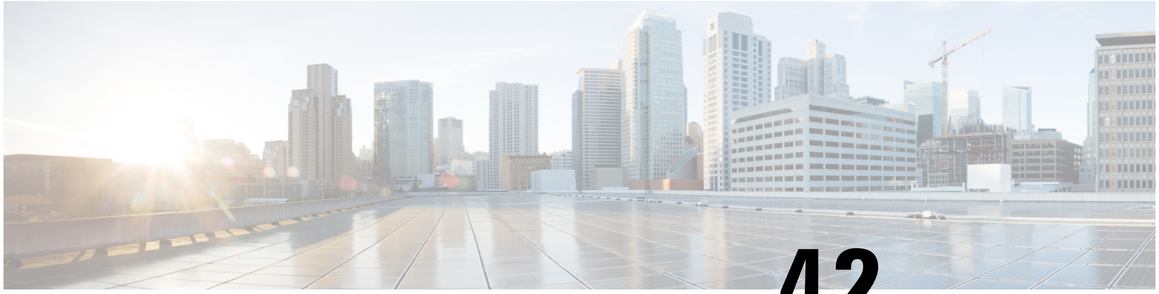
Protocol State Troubleshooting

The E-LMI line protocol state is reported in the “Line Protocol State” or “LineP State” fields in the output of forms of the **show ethernet lmi interfaces** command. The line protocol state is the state of the E-LMI protocol on the physical interface.

To investigate a line protocol state other than Up, consider the following guidelines:

- Admin-Down—The interface is configured with the **shutdown** command. Use the **no shutdown** command to bring the interface up.
- Down—Indicates a fault on the interface. Run the **show interfaces** command to display both the interface state and the interface line protocol state for more information, and take the following actions to investigate further:
  - If both states are Down, this suggests a physical problem with the link (for example, the cable is not plugged into either the PE or CE device).

- If the interface state is Up but the line protocol state is Down, this suggests that an OAM protocol has brought the line protocol state down due to a fault. Use the **show efd interface** command for more information.



CHAPTER 42

MPLS Traffic Engineering

This chapter provides conceptual and configuration information for the following MPLS-TE features:

- MPLS-TE Automatic Bandwidth
- MPLS-TE Fast Reroute (FRR)

Overview of MPLS Traffic Engineering

MPLS-TE software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what now can be achieved only by overlaying a Layer 3 network on a Layer 2 network.

MPLS-TE is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures. MPLS-TE provides an integrated approach to traffic engineering. With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

Benefits of MPLS-TE

MPLS-TE enables ISPs to route network traffic to offer the best service to their users in terms of throughput and delay. By making the service provider more efficient, traffic engineering reduces the cost of the network.

Currently, some ISPs base their services on an overlay model. In the overlay model, transmission facilities are managed by Layer 2 switching. The routers see only a fully meshed virtual topology, making most destinations appear one hop away. If you use the explicit Layer 2 transit layer, you can precisely control how traffic uses available bandwidth. However, the overlay model has numerous disadvantages. MPLS-TE achieves the TE benefits of the overlay model without running a separate network and without a non-scalable, full mesh of router interconnects.

How MPLS-TE works

MPLS-TE automatically establishes and maintains label switched paths (LSPs) across the backbone by using RSVP. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth. Available resources are flooded by means of extensions to a link-state-based Interior Gateway Protocol (IGP).

MPLS-TE tunnels are calculated at the LSP headend router, based on a fit between the required and available resources (constraint-based routing). The IGP automatically routes the traffic to these LSPs.

MPLS-TE Scale Details

Scale details for MPLS-TE:

Table 41: Supported LSPs for MPLS-TE

MPLS TE with FRR	Head/Tail Node: 75000 LSPs Mid Node: 37500 LSPs
MPLS TE without FRR	Head/Tail Node: 75000 LSPs Mid Node: 75000 LSPs

MPLS-TE Automatic Bandwidth

The MPLS-TE automatic bandwidth feature measures the traffic in a tunnel and periodically adjusts the signaled bandwidth for the tunnel.

MPLS-TE Automatic Bandwidth Overview

MPLS-TE automatic bandwidth is configured on individual Label Switched Paths (LSPs) at every head-end. MPLS-TE monitors the traffic rate on a tunnel interface. Periodically, MPLS-TE resizes the bandwidth on the tunnel interface to align it closely with the traffic in the tunnel. MPLS-TE automatic bandwidth can perform these functions:

- Monitors periodic polling of the tunnel output rate
- Resizes the tunnel bandwidth by adjusting the highest rate observed during a given period

For every traffic-engineered tunnel that is configured for an automatic bandwidth, the average output rate is sampled, based on various configurable parameters. Then, the tunnel bandwidth is readjusted automatically based upon either the largest average output rate that was noticed during a certain interval, or a configured maximum bandwidth value.

This table lists the automatic bandwidth functions.

Table 42: Automatic Bandwidth Variables

Function	Command	Description	Default Value
Application frequency	**application** command	Configures how often the tunnel bandwidths changed for each tunnel. The application period is the period of A minutes between the bandwidth applications during which the output rate collection is done.	24 hours
Requested bandwidth	**bw-limit** command	Limits the range of bandwidth within the automatic-bandwidth feature that can request a bandwidth.	0 Kbps
Collection frequency	**auto-bw collect** command	Configures how often the tunnel output rate is polled globally for all tunnels.	5 min
Highest collected bandwidth	—	You cannot configure this value.	—
Delta	—	You cannot configure this value.	—

The output rate on a tunnel is collected at regular intervals that are configured by using the **application** command in MPLS-TE auto bandwidth interface configuration mode. When the application period timer expires, and when the difference between the measured and the current bandwidth exceeds the adjustment threshold, the tunnel is reoptimized. Then, the bandwidth samples are cleared to record the new largest output rate at the next interval.

When reoptimizing the LSP with the new bandwidth, a new path request is generated. If the new bandwidth is not available, the last good LSP continues to be used. This way, the network experiences no traffic interruptions.

If minimum or maximum bandwidth values are configured for a tunnel, the bandwidth, which the automatic bandwidth signals, stays within these values.

Note When more than 100 tunnels are **auto-bw** enabled, the algorithm will jitter the first application of every tunnel by a maximum of 20% (max 1hour). The algorithm does this to avoid too many tunnels running auto bandwidth applications at the same time.

If a tunnel is shut down, and is later brought again, the adjusted bandwidth is lost and the tunnel is brought back with the initial configured bandwidth. In addition, the application period is reset when the tunnel is brought back.

Adjustment Threshold

Adjustment Threshold is defined as a percentage of the current tunnel bandwidth and an absolute (minimum) bandwidth. Both thresholds must be fulfilled for the automatic bandwidth to resignal the tunnel. The tunnel bandwidth is resized only if the difference between the largest sample output rate and the current tunnel bandwidth is larger than the adjustment thresholds.

For example, assume that the automatic bandwidth is enabled on a tunnel in which the highest observed bandwidth B is 30 Mbps. Also, assume that the tunnel was initially configured for 45 Mbps. Therefore, the difference is 15 mbit/s. Now, assuming the default adjustment thresholds of 10% and 10kbps, the tunnel is signalled with 30 Mbps when the application timer expires. This is because 10% of 45Mbit/s is 4.5 Mbit/s, which is smaller than 15 Mbit/s. The absolute threshold, which by default is 10kbps, is also crossed.

Overflow Detection

Overflow detection is used if a bandwidth must be resized as soon as an overflow condition is detected, without having to wait for the expiry of an automatic bandwidth application frequency interval.

For overflow detection one configures a limit N, a percentage threshold Y% and optionally, a minimum bandwidth threshold Z. The percentage threshold is defined as the percentage of the actual signalled tunnel bandwidth. When the difference between the measured bandwidth and the actual bandwidth are both larger than Y% and Z threshold, for N consecutive times, then the system triggers an overflow detection.

The bandwidth adjustment by the overflow detection is triggered only by an increase of traffic volume through the tunnel, and not by a decrease in the traffic volume. When you trigger an overflow detection, the automatic bandwidth application interval is reset.

By default, the overflow detection is disabled and needs to be manually configured.

Underflow Detection

Underflow detection is used when the bandwidth on a tunnel drops significantly, which is similar to overflow but in reverse.

Underflow detection applies the highest bandwidth value from the samples which triggered the underflow. For example, if you have an underflow limit of three, and the following samples trigger the underflow for 10 kbps, 20 kbps, and 15 kbps, then, 20 kbps is applied.

Unlike overflow, the underflow count is not reset across an application period. For example, with an underflow limit of three, you can have the first two samples taken at the end of an application period and then the underflow gets triggered by the first sample of the next application period.

Restrictions for MPLS-TE Automatic Bandwidth

When the automatic bandwidth cannot update the tunnel bandwidth, the following restrictions are listed:

- Tunnel is in a fast reroute (FRR) backup, active, or path protect active state. This occurs because of the assumption that protection is a temporary state, and there is no need to reserve the bandwidth on a backup tunnel. You should prevent taking away the bandwidth from other primary or backup tunnels.

- Reoptimization fails to occur during a lockdown. In this case, the automatic bandwidth does not update the bandwidth unless the bandwidth application is manually triggered by using the **mpls traffic-eng auto-bw apply** command in EXEC mode.

Configure Automatic Bandwidth

Configuring automatic bandwidth involves the following tasks:

- Configuring Collection Frequency
- Forcing the current application period to expire immediately
- Configuring the automatic bandwidth functions

Configure Collection Frequency

Perform this task to configure the collection frequency. You can configure only one global collection frequency.

Procedure

Step 1 **configure**

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname(config)# mpls traffic-eng
RP/0/RP0:hostname(config-mpls-te)#
```

Enters MPLS-TE configuration mode.

Step 3 **auto-bw collect frequency** *minutes*

Example:

```
RP/0/RP0:hostname(config-mpls-te)# auto-bw collect frequency 1
```

Configures the automatic bandwidth collection frequency, and controls the manner in which the bandwidth for a tunnel collects output rate information; but does not adjust the tunnel bandwidth.

minutes

Configures the interval between automatic bandwidth adjustments in minutes. Range is from 1 to 10080.

Step 4 **commit**

Forcing the Current Application Period to Expire Immediately

Perform this task to force the current application period to expire immediately on the specified tunnel. The highest bandwidth is applied on the tunnel before waiting for the application period to end on its own.

Procedure

Step 1 **mpls traffic-eng auto-bw apply** {**all** | **tunnel-te** *tunnel-number*}

Example:

```
RP/0/RP0:hostname# mpls traffic-eng auto-bw apply tunnel-te 1
```

Configures the highest bandwidth available on a tunnel without waiting for the current application period to end.

all

Configures the highest bandwidth available instantly on all the tunnels.

tunnel-te

Configures the highest bandwidth instantly to the specified tunnel. Range is from 0 to 65535.

Step 2 **commit**

Step 3 **show mpls traffic-eng tunnels** [**auto-bw**]

Example:

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

Displays information about MPLS-TE tunnels for the automatic bandwidth.

Configure Automatic Bandwidth Functions

Perform this task to configure the following automatic bandwidth functions:

Application frequency

Configures the application frequency in which a tunnel bandwidth is updated by the automatic bandwidth.

Bandwidth collection

Configures only the bandwidth collection.

Bandwidth parameters

Configures the minimum and maximum automatic bandwidth to set on a tunnel.

Adjustment threshold

Configures the adjustment threshold for each tunnel.

Overflow detection

Configures the overflow detection for each tunnel.

Procedure

Step 1 **configure**

Step 2 **interface tunnel-te** *tunnel-id*

Example:

```
RP/0/RP0:hostname(config)# interface tunnel-te 6
RP/0/RP0:hostname(config-if)#
```

Configures an MPLS-TE tunnel interface and enables traffic engineering on a particular interface on the originating node.

Step 3 **auto-bw**

Example:

```
RP/0/RP0:hostname(config-if)# auto-bw
RP/0/RP0:hostname(config-if-tunte-autobw)#
```

Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.

Step 4 **application** *minutes*

Example:

```
RP/0/RP0:hostname(config-if-tunte-autobw)# application 1000
```

Configures the application frequency in minutes for the applicable tunnel.

minutes

Frequency in minutes for the automatic bandwidth application. Range is from 5 to 10080 (7 days). The default value is 1440 (24 hours).

Step 5 **bw-limit** {**min** *bandwidth* } {**max** *bandwidth*}

Example:

```
RP/0/RP0:hostname(config-if-tunte-autobw)# bw-limit min 30 max 80
```

Configures the minimum and maximum automatic bandwidth set on a tunnel.

min

Applies the minimum automatic bandwidth in kbps on a tunnel. Range is from 0 to 4294967295.

max

Applies the maximum automatic bandwidth in kbps on a tunnel. Range is from 0 to 4294967295.

Step 6 **adjustment-threshold** *percentage* [**min** *minimum-bandwidth*]

Example:

```
RP/0/RP0:hostname(config-if-tunte-autobw)# adjustment-threshold 50 min 800
```

Configures the tunnel bandwidth change threshold to trigger an adjustment.

percentage

Bandwidth change percent threshold to trigger an adjustment if the largest sample percentage is higher or lower than the current tunnel bandwidth. Range is from 1 to 100 percent. The default value is 5 percent.

min

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. Range is from 10 to 4294967295 kilobits per second (kbps). The default value is 10 kbps.

Step 7 **overflow threshold** *percentage* [**min** *bandwidth*] **limit** *limit*

Example:

```
RP/0/RP0:hostname(config-if-tunte-autobw)# overflow threshold 100 limit 1
```

Configures the tunnel overflow detection.

percentage

Bandwidth change percent to trigger an overflow. Range is from 1 to 100 percent.

limit

Configures the number of consecutive collection intervals that exceeds the threshold. The bandwidth overflow triggers an early tunnel bandwidth update. Range is from 1 to 10 collection periods. The default value is none.

min

Configures the bandwidth change value in kbps to trigger an overflow. Range is from 10 to 4294967295. The default value is 10.

Step 8 **commit**

Fast Reroute

Table 43: Feature History

Feature Name	Release Information	Feature Description
Traffic Engineering (TE) over LAG	Cisco IOS XR Release 6.5.31	This feature allows the MPLS-TE tunnels to be protected with Fast Reroute (FRR) for interfaces on the LAG. If the LSPs in the MPLS-TE tunnel encounter a failed link, FRR reroutes the traffic carried by the LSPs. Commands added: • show mpls traffic-eng fast-reroute database • show mpls traffic-eng fast-reroute log

Fast Reroute (FRR) provides link protection to LSPs enabling the traffic carried by LSPs that encounter a failed link to be rerouted around the failure. The reroute decision is controlled locally by the router connected to the failed link. The headend router on the tunnel is notified of the link failure through IGP or through RSVP. When it is notified of a link failure, the headend router attempts to establish a new LSP that bypasses the failure. This provides a path to reestablish links that fail, providing protection to data transfer.

You should be aware of these requirements for the backup tunnel path

- Backup tunnel must not pass through the element it protects.
- Primary tunnel and a backup tunnel should intersect at least at two points (nodes) on the path: point of local repair (PLR) and merge point (MP). PLR is the headend of the backup tunnel, and MP is the tailend of the backup tunnel.

Note When you configure TE tunnel with multiple protection on its path and merge point is the same node for more than one protection, you must configure record-route for that tunnel.

FRR Node Protection

If a link failure occurs within an area, the upstream router directly connected to the failed link generates an RSVP path error message to the headend. As a response to the message, the headend sends an RSVP path tear message and the corresponding path option is marked as invalid for a specified period and the next path-option (if any) is evaluated.

To retry the ABR immediately, a second path option (identical to the first one) should be configured. Alternatively, the retry period (path-option hold-down, 2 minutes by default) can be tuned to achieve a faster retry.

Protecting MPLS Tunnels with Fast Reroute

From R6.5.3.1, the MPLS tunnels can be protected with Fast Reroute for LAG interfaces.

Before you begin

The following prerequisites are required to protect MPLS-TE tunnels:

- You must have a router ID for the neighboring router.
- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.
- You must first configure a primary tunnel.

Procedure

Step 1 **configure**

Step 2 **interface tunnel-te** *tunnel-id*

Example:

```
RP/0/RP0:hostname# interface tunnel-te 1
```

Configures an MPLS-TE tunnel interface.

Step 3 **fast-reroute**

Example:

```
RP/0/RP0:hostname(config-if)# fast-reroute
```

Enables fast reroute.

Step 4 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits the current configuration mode.

Step 5 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname(config)# mpls traffic-eng
```

```
RP/0/RP0:hostname(config-mpls-te)#
```

Enters MPLS-TE configuration mode.

Step 6 **reoptimize timers delay {cleanup** *delay-time* **| installation** *delay-time***}**

Example:

```
RP/0/RP0:hostname(config-mpls-te)# reoptimize timers delay cleanup 180
RP/0/RP0:hostname(config-mpls-te)# reoptimize timers delay installation 180
```

Delays removal of the old LSPs and installation of a new label after tunnel reoptimization. The minimum installation and cleanup time is 180 seconds.

Step 7 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-mpls-te)# interface TenGigE0/1/0/3
RP/0/RP0:hostname(config-mpls-te-if)#
```

Example:

```
RP/0/RP0:hostname(config-mpls-te)# interface bundle-ether 150
RP/0/RP0:hostname(config-mpls-te-if)#
```

Enables traffic engineering on a particular interface on the originating node. From R6.5.3.1, you can also enable traffic engineering on LAG interface.

Step 8 **backup-path tunnel-te** *tunnel-number*

Example:

```
RP/0/RP0:hostname(config-mpls-te-if)# backup-path tunnel-te 2
```

Sets the backup path to the backup tunnel.

Step 9 **exit**

Example:

```
RP/0/RP0:hostname(config-mpls-te-if)# exit
RP/0/RP0:hostname(config-mpls-te)#
```

Exits the current configuration mode.

Step 10 **exit**

Example:

```
RP/0/RP0:hostname(config-mpls-te)# exit
RP/0/RP0:hostname(config)#
```

Exits the current configuration mode.

Step 11 **interface tunnel-te** *tunnel-id*

Example:

```
RP/0/RP0:hostname(config)# interface tunnel-te 2
```

Configures an MPLS-TE tunnel interface.

Step 12 **ipv4 unnumbered** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-if)# ipv4 unnumbered Loopback0
```

Assigns a source address to set up forwarding on the new tunnel.

Step 13 **path-option** *preference-priority* {**explicit name** *explicit-path-name*}

Example:

```
RP/0/RP0:hostname(config-if)# path-option l explicit name backup-path
```

Sets the path option to explicit with a given name (previously configured) and assigns the path ID.

Step 14 **destination** *ip-address*

Example:

```
RP/0/RP0:hostname(config-if)# destination 192.168.92.125
```

Assigns a destination address on the new tunnel.

- Destination address is the remote node’s MPLS-TE router ID.
- Destination address is the merge point between backup and protected tunnels.

Note When you configure TE tunnel with multiple protection on its path and merge point is the same node for more than one protection, you must configure record-route for that tunnel.

Step 15 **commit**

Step 16 (Optional) **show mpls traffic-eng tunnels backup**

Example:

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

Displays the backup tunnel information.

Step 17 (Optional) **show mpls traffic-eng tunnels protection frr**

Example:

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

Displays the tunnel protection information for Fast-Reroute (FRR).

Step 18 (Optional) **show mpls traffic-eng fast-reroute database**

Example:

```
RP/0/RP0:hostname# show mpls traffic-eng fast-reroute database
```

Displays the protected tunnel state (for example, the tunnel’s current ready or active state).

Step 19 (Optional) **show mpls traffic-eng fast-reroute log**

Example:

```
RP/0/RP0:hostname# show mpls traffic-eng fast-reroute log
```

Displays the log of FRR events.

Path Computation Client Initiated RSVP-TE

Table 44: Feature History

Feature Name	Release Information	Feature Description
Path Computation Client Initiated RSVP-TE	Cisco IOS XR Release 6.5.31	This feature establishes Path Computation Element Communication Protocol (PCEP) between PCE (NCS 5500) and Path Computation Client (PCC) (NCS 4000) and creates RSVP-TE tunnels between the head end node (PCC) and a tail end node (another NCS 4000 device). It supports client such as Cisco Optimization Engine (COE) to preview the RSVP-TE path initiated by PCC, before deployment, thereby supporting Bandwidth on Demand (BWoD). Commands added: • show pce ipv4 • show pce lps • show mpls traffic-eng pce peer • show mpls traffic-eng pce lsp-database

Cisco IOS-XR Path Computation Element (PCE) collects network topology through IGP and/or BGP-LS, and provides path computation services for RSVP-TE tunnels. Also, it supports any external client (for example, Cisco Crosswork Optimization Engine (COE)) to deploy RSVP-TE tunnels based on the client’s needs. COE obtains services such as topology collection, path computation, and RSVP-TE deployment services from PCE, to support Bandwidth on Demand (BWoD) and Bandwidth Optimization (BWOpt) applications.

PCE describes a set of procedures by which a Path Computation Client (PCC) can report and delegate control of head end tunnels that are sourced from the PCC to a PCE peer. The PCC and PCE establish a PCE Communication Protocol (PCEP) connection that PCE uses to push updates to the network.

About RSVP-TE tunnels, PCE support is restricted to disjoint path computation (node, link, SRLG). Also, RSVP-TE tunnels reports to PCE for discovery purpose.

From Release 7.3.1, the following features in PCE and PCC support clients such as COE, WAE, or any third-party tools:

- Clients can discover RSVP-TE tunnels that are delegated or simply reported to PCE.
- Neither PCE nor client can modify the path of a nondelegated tunnel.
- PCE always dynamically computes the path of a delegated tunnel that is initiated by PCC, and clients cannot modify the paths.
- Clients can preview an RSVP-TE path before deployment. Clients may also choose not to deploy that tunnel.

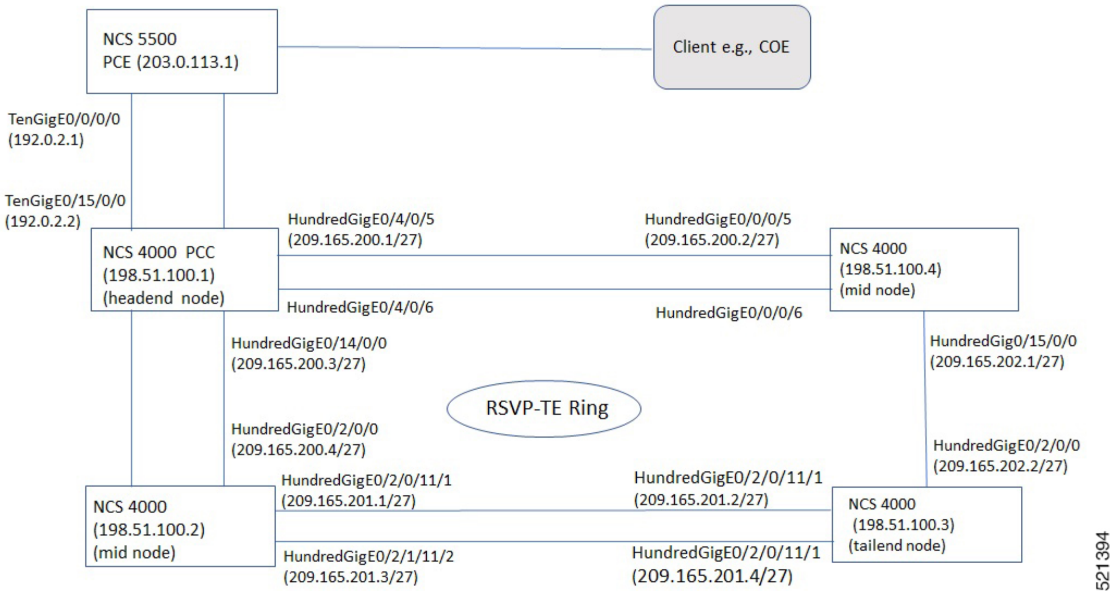
PCC runs on NCS 4000 and the PCE runs on the platforms such as ASR 9000, XRv9000, and NCS 5500 where the software should be 6.6.3+optima1.1SMU or higher, up where the PCE support for optima1.1 exists.

Limitations

PCE supports low latency, low cost, disjoint path computation with affinity and bandwidth constraints. Affinity and disjoint constraints are not supported.

Use Case - PCC-Initiated RSVP-TE for BWoD

The following topology explains the workflow for initiating delegated RSVP-TE tunnel for the BWoD application:



The topology has four NCS 4000 nodes for redundancy and one NCS 5500 node (PCE). The headend node (198.51.100.1) is connected to PCE (203.0.113.1) through the interface. Perform the following steps to create an RSVP-TE tunnel between the headend node (198.51.100.1) and the tailend node (198.51.100.3).

Procedure

Step 1 Check whether the IS-IS interfaces of the NCS 4000 nodes (headend, mid node, tailend) are up and running using the following command:

```
RP/0/RP0:NCS4016-1#show ip interface brief
Tue Feb 9 12:14:34.807 IST

Interface                IP-Address       Status      Protocol      Vrf-Name
Bundle-Ether12           unassigned       Down        Down          default
Loopback5000             198.51.100.1          Up          Up            default
HundredGigE0/0/0/5       unassigned       Down        Down          default
HundredGigE0/0/0/5.100   85.1.1.1         Down        Down          default
HundredGigE0/0/0/10/1    unassigned       Down        Down          default
HundredGigE0/2/0/5       unassigned       Up          Up            default
HundredGigE0/2/0/5.100   6198.51.100.1         Up          Up            default
HundredGigE0/4/0/5       20.20.20.2       Up          Up            default
HundredGigE0/4/0/5.100   14.1.1.1         Up          Up            default
HundredGigE0/4/0/6       unassigned       Down        Down          default
HundredGigE0/13/0/10/1   unassigned       Up          Up            default
HundredGigE0/14/0/0      17.0.0.1         Up          Up            default
HundredGigE0/14/0/0.100  12.1.2.1         Up          Up            default
HundredGigE0/14/0/11/1   13.1.1.1         Down        Down          default
HundredGigE0/15/0/0      unassigned       Shutdown    Down          default
FortyGigE0/15/0/8        24.0.0.1         Up          Up            default
TenGigE0/15/0/5/1        192.168.1.1      Up          Up            default
TenGigE0/15/0/5/2        unassigned       Shutdown    Down          default
TenGigE0/15/0/5/3        unassigned       Shutdown    Down          default
TenGigE0/15/0/5/4        unassigned       Shutdown    Down          default
MgmtEth0/RP0/CPU0/0      10.58.230.71     Up          Up            default
MgmtEth0/RP0/EMS/0       unassigned       Up          Up            default
MgmtEth0/RP0/CRAFT/0     unassigned       Shutdown    Down          default
MgmtEth0/RP1/CPU0/0      10.58.230.69     Shutdown    Down          default
MgmtEth0/RP1/EMS/0       unassigned       Shutdown    Down          default
MgmtEth0/RP1/CRAFT/0     unassigned       Shutdown    Down          default
RP/0/RP0:NCS4016-1#
```

Step 2 If any interface is down, use the following command to make the interface up and running:

```
RP/0/RP1:NCS4016-1#configure
RP/0/RP1:NCS4016-1(config)#controller optics 0/15/0/1
RP/0/RP1:NCS4016-1(config-Optics)#no shutdown
RP/0/RP1:NCS4016-1(config-Optics)#commit
```

Step 3 Configure the NCS 5500 for PCE:

Table 45:

Configuration	Commands
1. Assign IP address to the interface and configure static routing with the NCS 4000 headend node.	interface Loopback0 ipv4 address 203.0.113.1 255.255.255.255 ! interface MgmtEth0/RP0/CPU0/0 ipv4 address 10.58.230.130 255.255.0.interface TenGigE0/0/0/0 ipv4 address 192.0.2.1 255.255.255.0 ! router static address-family ipv4 unicast 0.0.0.0/0 10.58.228.1 198.51.100.1/32 192.0.2.2
2. Configure iBGP protocol	router bgp 1 bgp router-id 203.0.113.1 address-family ipv4 unicast network 203.0.113.1/32 ! address-family link-state link-state ! neighbor 198.51.100.1 remote-as 1 update-source Loopback0 address-family ipv4 unicast ! address-family link-state link-state
3.Configure PCE	pce address ipv4 203.0.113.1 api user cisco password encrypted 00071A15075 ! ! timers minimum-peer-keepalive 0

Step 4 Configure the NCS 4000 headend and tailend nodes:

Table 46:

Configuration	NCS 4000 (Headend node - PCC)	NCS 4000 (Tailend node)
1. Configure the Interface	Loopback Configuration interface Loopback5000 ipv4 address 198.51.100.1 255.255.255.255 Headend to mid node1 configuration interface HundredGigE0/14/0/0 ipv4 address 209.165.200.3 255.255.255.0 load-interval 30 Headend to PCE configuration interface TenGigE0/15/0/5/1 ipv4 address 192.0.2.2 255.255.255.0 Headend to mid node2 configuration interface HundredGigE0/4/0/5 ipv4 address 209.165.200.1 255.255.255.0 load-interval 30	Loopback Configuration interface Loopback9000 ipv4 address 198.51.100.3 255.255.255.255 Tailend to mid node2 configuration interface HundredGigE0/2/0/11/1 mtu 9600 ipv4 address 209.165.201.2 0.3255.255.255.252 load-interval 30 Tailend to mid node2 configuration interface HundredGigE0/2/0/0 mtu 9600 ipv4 address 209.165.202.2 255.255.255.0 load-interval 30
2. Configure IGP (IS-IS)	router isis 100 is-type level-2-only net 49.2001.1000.0100.1001.00 nsr distribute link-state nsf cisco log adjacency changes address-family ipv4 unicast metric-style wide mpls traffic-eng level-2-only mpls traffic-eng router-id Loopback5000 router-id 198.51.100.1 ! interface Loopback5000 passive address-family ipv4 unicast ! ! interface HundredGigE0/4/0/5 circuit-type level-2-only point-to-point address-family ipv4 unicast ! ! interface HundredGigE0/14/0/0 point-to-point address-family ipv4 unicast ! ! interface HundredGigE0/14/0/0 point-to-point address-family ipv4 unicast	router isis 100 is-type level-2-only net 47.0001.0000.0000.0009.00 nsr distribute link-state level 2 nsf cisco log adjacency changes address-family ipv4 unicast metric-style wide mpls traffic-eng level-2-only mpls traffic-eng router-id Loopback9000 ! interface Loopback9000 address-family ipv4 unicast ! ! interface HundredGigE0/2/0/0 point-to-point address-family ipv4 unicast ! interface HundredGigE0/2/0/11/1 point-to-point address-family ipv4 unicast ! ! !

Configuration	NCS 4000 (Headend node - PCC)	NCS 4000 (Tailend node)

3. Configure BGP (iBGP)	`router bgp 1`
	` bgp router-id 198.51.100.1`
	` address-family ipv4 unicast`
	` !`
	` address-family link-state link-state`
	` !`
	` neighbor 198.51.100.3`
	`  remote-as 1`
	`  update-source Loopback5000`
	`  address-family ipv4 labeled-unicast`
	`   route-reflector-client`
	`   next-hop-self`
	`  !`
	` !`
	`neighbor 203.0.113.1`
	`  remote-as 1`
	`  update-source Loopback5000`
	`  address-family ipv4 unicast`
	`  !`
	`  address-family link-state link-state`
	`  !`
	` !`
	` neighbor 11.11.11.11`
	`  remote-as 1`
	`  update-source Loopback5000`
	`  address-family ipv4 unicast`
	`  !`
	`  address-family link-state link-state`
	`  !`
	` !`
	`!`
		`router bgp 1`
		` bgp router-id 198.51.100.3`
		` ibgp policy out enforce-modifications`
		` address-family ipv4 unicast`
		`  allocate-label all`
		` !`
		` address-family link-state link-state`
		` !`
		` neighbor 198.51.100.1`
		`  remote-as 1`
		`  update-source Loopback9000`
		`  address-family ipv4 labeled-unicast`
		`   route-reflector-client`
		`   next-hop-self`
		`  !`
		`  address-family link-state link-state`
		`  !`
		` !`
		`!`

4. Configure RSVP	`rsvp`
	` interface HundredGigE0/0/0/5`
	`  bandwidth percentage 99`
	` !`
	` interface HundredGigE0/4/0/5`
	`  bandwidth percentage 99`
	` !`
	` interface HundredGigE0/14/0/0`
	`  bandwidth percentage 99`
	` !`
	` latency threshold 100`
	`!`
		`rsvp`
		` interface HundredGigE0/0/0/5`
		`  bandwidth percentage 99`
		` !`
		` interface HundredGigE0/15/0/0`
		`  bandwidth percentage 99`
		` !`
		`!`

5. Configure MPLS-TE	`mpls traffic-eng`
	` interface HundredGigE0/0/0/5`
	` !`
	` interface HundredGigE0/4/0/5`
	`  auto-tunnel backup`
	`  !`
	` !`
	` interface HundredGigE0/14/0/0`
	`  auto-tunnel backup`
	`  !`
	` !`
		`mpls traffic-eng`
		` interface HundredGigE0/2/0/0`
		` !`
		` interface HundredGigE0/2/0/11/1`
		` !`
		` fault-oam`
		` signalling advertise explicit-null`
		
		` path-selection`
		`  metric igp`
		` !`
		`!`

Configuration	NCS 4000 (Headend node - PCC)	NCS 4000 (Tailend node)

6. Establish PCEP session with PCE	pce
	peer source ipv4 198.51.100.1
	  peer ipv4 203.0.113.1
	   precedence 10
	  !
	  peer ipv4 11.11.11.11
	   precedence 20
	  !
	  logging events peer-status
	  stateful-client
	   instantiation
	   report
	   timers state-timeout 600
	   redundancy pcc-centric
	  !
	 !
	 auto-tunnel pcc
	  tunnel-id min 5000 max 7000
	 !
	 fault-oam
	 signalling advertise explicit-null
	 path-selection
	  metric igp
	 !
	!
		Not applicable for tail end configuration.

7. MPLS-TE TUNNEL Configuration	interface tunnel-te300 description PCEP-TEST bandwidth 100 destination 198.51.100.3 fast-reroute protect bandwidth path-protection protection-mode non-revertive ! path-option 1 dynamic pce delegation ! ! !	Not applicable for tail end configuration.

Step 5 Configure the NCS 4000 mid nodes:

Table 47:

Configuration	NCS 4000 (mid node 1)	NCS 4000 (mid node 2)
Interface	interface Loopback8000 ipv4 address 198.51.100.2 255.255.255.255 ! interface HundredGigE0/2/0/0 mtu 9600 ipv4 address 209.165.200.4 255.255.255.0 load-interval 30 ! interface HundredGigE0/2/0/11/1 mtu 9600 ipv4 address 209.165.201.1 255.255.255.0 load-interval 30 !	interface Loopback7000 ipv4 address 198.51.100.4 255.255.255.255 ! interface HundredGigE0/0/0/5 ipv4 address 209.165.200.2 255.255.255.0 load-interval 30 ! interface HundredGigE0/15/0/0 mtu 9600 ipv4 address 209.165.202.1 255.255.255.0 !
IGP (IS-IS)	router isis 100 is-type level-2-only net 47.0001.0000.0000.0008.00 nsr distribute link-state level 2 nsf cisco log adjacency changes address-family ipv4 unicast metric-style wide mpls traffic-eng level-2-only mpls traffic-eng router-id Loopback8000 ! interface Loopback8000 address-family ipv4 unicast ! ! interface HundredGigE0/2/0/0 point-to-point address-family ipv4 unicast	router isis 100 is-type level-2-only net 47.0001.0000.0000.0010.00 nsr nsf cisco log adjacency changes address-family ipv4 unicast metric-style wide mpls traffic-eng level-2-only mpls traffic-eng router-id Loopback7000 ! interface Loopback7000 address-family ipv4 unicast ! ! interface HundredGigE0/0/0/5 point-to-point address-family ipv4 unicast ! ! interface HundredGigE0/15/0/0 point-to-point address-family ipv4 unicast ! ! !
RSVP	rsvp interface HundredGigE0/2/0/0 bandwidth percentage 99 ! interface HundredGigE0/2/0/11/1 bandwidth percentage 99 !	rsvp interface HundredGigE0/0/0/5 bandwidth percentage 99 ! interface HundredGigE0/15/0/0 bandwidth percentage 99 ! !

Configuration	NCS 4000 (mid node 1)	NCS 4000 (mid node 2)
MPLS TE	mpls traffic-eng interface HundredGigE0/2/0/0 ! interface HundredGigE0/2/0/11/1 ! fault-oam signalling advertise explicit-null path-selection metric igp !	mpls traffic-eng interface HundredGigE0/0/0/5 ! interface HundredGigE0/15/0/0 ! fault-oam signalling advertise explicit-null path-selection metric igp ! !

Step 6 Log in to a server installed with CURL and execute the following command, so that PCE initiates the RSVP-TE tunnel provisioning:

```
bash-4.2$ curl --raw -vN "http://cisco:cisco@10.77.142.23:8080/lsp/create/
simple?allow-xtc-reoptimization=1&name=l&source=198.51.100.1&destination=198.51.100.3&peer=198.51.100.1&metric-latency=20&type=rsvp"
* About to connect() to 10.77.142.23 port 8080 (#0)
* Trying 10.77.142.23...
* Connected to 10.77.142.23 (10.77.142.23) port 8080 (#0)
* Server auth using Basic with user 'cisco'
> GET
/lsp/create/simple?allow-xtc-reoptimization=1&name=l&source=198.51.100.1&destination=198.51.100.3
&peer=198.51.100.1&metric-latency=20&type=rsvp HTTP/1.1
> Authorization: Basic Y2lzY286Y2lzY28=
> User-Agent: curl/7.29.0
Host: 10.77.142.23:8080
Accept: */*
>
< HTTP/1.1 200 OK
< Cache-Control: no-cache, no-store
< Content-Type: text/json; charset=utf-8
< Expires: -1
< Transfer-Encoding: chunked
< Connection: keep-alive
<
30
create-lsp "l" (rsvp) on peer 198.51.100.1 (Success)
0
* Connection #0 to host 10.77.142.23 left intact
```

Step 7 Verify if the RSVP-TE tunnel is created, using the **show mpls traffic-eng** command:

```
RP/0/RP1:NCS4016-1#show mpls traffic-eng tunnels tabular
Tunnel             LSP    Destination     Source        Tun      FRR         LSP    Path
Name               ID     Address         Address       State    State       Role   Prot
--------------     -----  -------------  --------------- ------ ------ ---- -----
tunnel-te1          2     198.51.100.3    198.51.100.1    up     Ready    Headend   Inact
*tunnel-te8240      4     198.51.100.2    198.51.100.1    up     Inact    Headend   Inact
*tunnel-te8260      0     198.51.100.3    0.0.0.0         down   Inact    Headend   Inact
NCS4016-3 tl        6     198.51.100.1    198.51.100.3    up     Inact    Tailend
Autob NCS4009-2 t   2     198.51.100.1    198.51.100.2    up     Inact    Tailend
*= automatically created backup tunnel
```

Step 8 Verify the detailed information of the RSVP-TE tunnel, using the **show mpls traffic-eng** command:

```
   RP/0/RP0:NCS4016-1#show mpls traffic-eng tunnels 300
Name: tunnel-te300  Destination: 198.51.100.3  Ifhandle:0x8800584
  Signalled-Name: PCEP-TEST
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected
    path option 10, (verbatim) type explicit (autopcc_te300) (Basis for Setup)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Thu Jul  2 12:28:37 2020 (4w0d ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: IGP (interface)
    Path Selection:
      Tiebreaker: Min-fill (default)
    Hop-limit: disabled
    Cost-limit: disabled
    Delay-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (not enabled)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Auto-Capacity: Disabled:
    Fast Reroute: Enabled, Protection Desired: Bandwidth
    Path Protection: Enabled
      Non-revertive
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    Soft Preemption: Disabled
PCE Delegation:
    Symbolic name: "PCEP-TEST"
    PCEP ID: 301
    Delegated to: 203.0.113.1
  History:
    Tunnel has been up for: 2d13h (since Mon Jul 27 23:30:10 IST 2020)
    Current LSP:
      Uptime: 1d03h (since Wed Jul 29 09:36:50 IST 2020)
    Prior LSP:
      ID: 124 Path Option: 10
      Removal Trigger: reoptimization completed
  Path info (PCE controlled):
  Hop0: 209.165.200.4
  Hop1: 51.0.0.2
Displayed 1 (of 2004) headends, 0 (of 0) midpoints, 0 (of 7) tailends
Displayed 1 up, 0 down, 0 recovering, 0 recovered headends
```

Step 9 Verify the PCE node peer address and state using the **show mpls traffic-eng pce peer** command:

```
RP/0/RP0:NCS4016-1#show mpls traffic-eng 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)\
```

Step 10 Check the LSP database of the tunnel using the **show mpls traffic-eng pce lsp-database** command:

```
RP/0/RP0:NCS4016-1#show mpls traffic-eng 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
```

Step 11 Verify PCEP session details using the **show pce ipv4 peer** command:

```
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
```

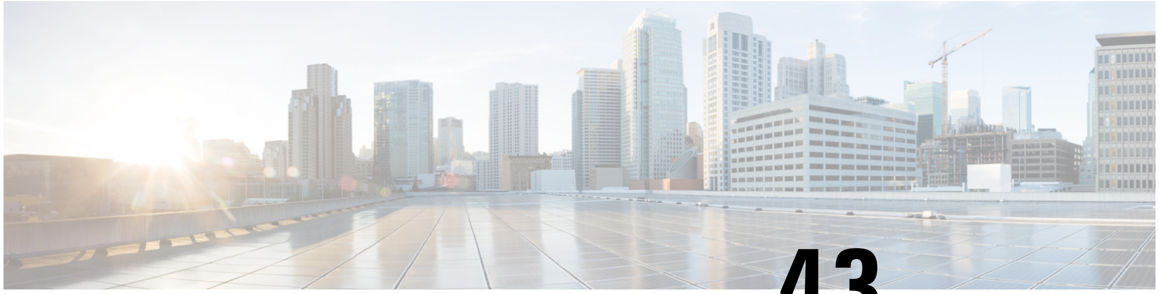
```
198.51.100.1       m1              0     198.51.100.1     198.51.100.3   5000   8      up
    up   PCE Initiated (CURL)
```

Step 12 View the summary of the PCE topology information using the **show pce ipv4 topology summary** command:

```
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
```

Step 13 View the detailed information of an LSP present in the PCE's LSP database, in table format using the **show pce lsp tabular** command:

```
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
```



CHAPTER 43

Configure Frequency Synchronization

This chapter describes the Cisco IOS XR commands to configure Frequency Synchronization.

Frequency Synchronization

Frequency synchronization is the ability to distribute precision frequency around the network. Precision frequency is required in the next generation networks for applications such as circuit emulation. To achieve compliance to ITU specifications for TDM, differential method circuit emulation must be used, which requires a known, common precision frequency reference at each end of the emulated circuit.

To maintain frequency synchronization links, a set of operations messages are required. These messages ensure a node is always deriving timing from the most reliable source, and transfers information about the quality of the timing source being used to clock the frequency synchronization link.

Configuring Frequency Synchronization

Enabling Frequency Synchronization on the Router

This task describes the router-level configurations required to enable frequency synchronization.

Procedure

Step 1 **configure**

Step 2 **frequency synchronization**

Example:

```
RP/0/RP0:hostname(config)# frequency synchronization
```

Enables frequency synchronization on the router.

Step 3 **clock-interface timing-mode system**

Example:

```
RP/0/RP0:hostname(config-freqsync)# clock-interface timing-mode system
```

Sets the timing source for clock-interface output.

Step 4 **quality itu-t option** {**1** | **2 generation** {**1** | **2**}}

Example:

```
RP/0/RP0:hostname(config-freqsync)# quality itu-t
option 2 generation 1
```

(Optional) Specifies the quality level for the router. The default is **option 1**.

- **option 1**—Includes PRC, SSU-A, SSU-B, SEC and DNU.
- **option 2 generation 1**—Includes PRS, STU, ST2, ST3, SMC, ST4, RES and DUS.
- **option 2 generation 2**—Includes PRS, STU, ST2, ST3, TNC, ST3E, SMC, ST4, PROV and DUS.

Note The quality option configured here must match the quality option specified in the **quality receive** and **quality transmit** commands in interface frequency synchronization configuration mode.

Step 5 **log selection** {**changes** | **errors**}

Example:

```
RP/0/RP0:hostname(config-freqsync)# log selection changes
```

Enables logging to frequency synchronization.

- **changes**—Logs every time when there is a change to the selected source, in addition to errors.
- **errors**—Logs only when there are no available frequency sources, or when the only available frequency source is the internal oscillator.

Step 6 Use one of these commands:

- **end**
- **commit**

Example:

```
RP/0/RP0:hostname(config-freqsync)# end
```

or

```
RP/0/RP0:hostname(config-freqsync)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

  ```
  Uncommitted changes found, commit them
  before exiting(yes/no/cancel)? [cancel]:
  ```

  - When you enter **`yes`**, it saves the configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - When you enter **`no`**, it exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

- When you enter **cancel**, it leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file, and remain within the configuration session.

What to do next

Configure frequency synchronization on any interface that should participate in Frequency Synchronization.

Configuring Frequency Synchronization on an Interface

By default, there is no frequency synchronization on line interfaces. Use this task to configure an interface to participate in Frequency Synchronization.

Limitations:

- Maximum two interfaces are monitored for frequency synchronization selection.
- Frequency Synchronization is supported only with the following:

Interface Type	Controller	Mapping Type
Ethernet packet (LAN PHY).	TenGigE, FortyGigE, and HundredGigE	N/A
Ethernet terminated non-channelized OTN.	OTU2e and OTU3	bmp
Ethernet terminated non-channelized OTN.	OTU4	gmp

Before you begin

You must enable frequency synchronization globally on the router.

Procedure

Step 1 **config**

Example:

```
RP/0/RP0:hostname# config
```

Enters configuration mode.

Step 2 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface tenGigE0/1/0/1
```

Enters interface configuration mode.

Step 3 **frequency synchronization**

Example:

```
RP/0/RP0:hostname(config-if)# frequency synchronization
```

Enters interface configuration mode.

Step 4 **selection input**

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# selection input
```

(Optional) Specifies the interface as a timing source to be passed to the selection algorithm.

Step 5 **priority** *priority-value*

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# priority 100
```

(Optional) Configures the priority of the frequency source on a controller or an interface. Values can range from 1 (highest priority) to 254 (lowest priority). The default value is 100.

This command is used to set the priority for an interface . The priority is used in the clock-selection algorithm to choose between two sources that have the same quality level (QL). Lower priority values are preferred.

Step 6 **wait-to-restore** *minutes*

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# wait-to-restore 3
```

(Optional) Configures the wait-to-restore time, in minutes, for frequency synchronization on an interface. This is the amount of time after the interface comes up before it is used for synchronization. Values can range from 0 to 12. The default value is 5.

Step 7 **ssm disable**

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# ssm disable
```

(Optional) Disables Synchronization Status Messages (SSMs) on the interface.

- For frequency synchronization interfaces, this disables sending ESMC packets, and ignores any received ESMC packets.

Step 8 **quality transmit** {**exact** | **highest** | **lowest**} **itu-t option** *ql-option*

Example:

```
RP/0/RP0:hostname(config-clk-freqsync)# quality transmit
highest itu-t option 1 prc
```

(Optional) Adjusts the QL that is transmitted in SSMs.

- **exact** *ql*—Specifies the exact QL to send, otherwise DNU will be send.
- **highest** *ql*—Specifies an upper limit on the received QL. The received QL will be used if the received value is higher than this specified QL.
- **lowest** *ql*—Specifies a lower limit on the received QL. DNU will be used if the received value is lower than this specified QL.

The quality option specified in this command must match the globally-configured quality option in the **quality itu-t option** command.

Step 9 **quality receive** {**exact** | **highest** | **lowest**} **itu-t option** *ql-option*

Example:

```
RP/0/RP0:hostname(config-clk-freqsync)# quality receive
highest itu-t option 1 prc
```

(Optional) Adjusts the QL value that is received in SSMs, before it is used in the selection algorithm.

- **exact** *ql*—Specifies the exact QL to send, otherwise DNU will be send.
- **highest** *ql*—Specifies an upper limit on the received QL. The received QL will be used if the received value is higher than this specified QL.
- **lowest** *ql*—Specifies a lower limit on the received QL. DNU will be used if the received value is lower than this specified QL.

The quality option specified in this command must match the globally-configured quality option in the **quality itu-t option** command.

Step 10 Use one of these commands:

- **end**
- **commit**

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# end
```

or

```
RP/0/RP0:hostname(config-if-freqsync)# commit
```

Saves configuration changes.

Configuring Frequency Synchronization on a Clock Interface

To enable a clock interface to be used as frequency input or output, you must configure the port parameters and frequency synchronization, as described in this task.

Note The configuration on clock interfaces must be the same for corresponding clock interfaces across all RP's to avoid changes in frequency synchronization behavior in the event of an RP switchover.

Procedure

Step 1 **configure**

Step 2 Perform to configure a clock interface.

Step 3 **ics**

Example:

```
RP/0/RP0:hostname(config)# ics
```

Enables chassis synchronization.

Step 4 **frequency synchronization**

Example:

```
RP/0/RP0:hostname(config-clock-if)# frequency synchronization
RP/0/RP0:hostname(config-clk-freqsync)#
```

Enters clock interface frequency synchronization mode to configure frequency synchronization parameters.

Note The remaining steps in this task are the same as those used to configure the interface frequency synchronization.

Step 5 **selection input**

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# selection input
```

(Optional) Specifies the interface as a timing source to be passed to the selection algorithm.

Step 6 **priority** *priority-value*

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# priority 100
```

(Optional) Configures the priority of the frequency source on a controller or an interface. Values can range from 1 (highest priority) to 254 (lowest priority). The default value is 100.

This command is used to set the priority for an interface . The priority is used in the clock-selection algorithm to choose between two sources that have the same quality level (QL). Lower priority values are preferred.

Step 7 **wait-to-restore** *minutes*

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# wait-to-restore 3
```

(Optional) Configures the wait-to-restore time, in minutes, for frequency synchronization on an interface. This is the amount of time after the interface comes up before it is used for synchronization. Values can range from 0 to 12. The default value is 5.

Step 8 **ssm disable**

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# ssm disable
```

(Optional) Disables Synchronization Status Messages (SSMs) on the interface.

- For frequency synchronization interfaces, this disables sending ESMC packets, and ignores any received ESMC packets.

Step 9 **quality transmit** {**exact** | **highest** | **lowest**} **itu-t option** *ql-option*

Example:

```
RP/0/RP0:hostname(config-clk-freqsync)# quality transmit
highest itu-t option 1 prc
```

(Optional) Adjusts the QL that is transmitted in SSMs.

- **exact** *ql*—Specifies the exact QL to send, otherwise DNU will be send.
- **highest** *ql*—Specifies an upper limit on the received QL. The received QL will be used if the received value is higher than this specified QL.
- **lowest** *ql*—Specifies a lower limit on the received QL. DNU will be used if the received value is lower than this specified QL.

The quality option specified in this command must match the globally-configured quality option in the **quality itu-t option** command.

Step 10 **quality receive** {**exact** | **highest** | **lowest**} **itu-t option** *ql-option*

Example:

```
RP/0/RP0:hostname(config-clk-freqsync)# quality receive
highest itu-t option 1 prc
```

(Optional) Adjusts the QL value that is received in SSMs, before it is used in the selection algorithm.

- **exact** *ql*—Specifies the exact QL to send, otherwise DNU will be send.
- **highest** *ql*—Specifies an upper limit on the received QL. The received QL will be used if the received value is higher than this specified QL.
- **lowest** *ql*—Specifies a lower limit on the received QL. DNU will be used if the received value is lower than this specified QL.

The quality option specified in this command must match the globally-configured quality option in the **quality itu-t option** command.

Step 11 Use one of these commands:

- **end**
- **commit**

Example:

```
RP/0/RP0:hostname(config-if-freqsync)# end
```

or

```
RP/0/RP0:hostname(config-if-freqsync)# commit
```

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

  ```
  Uncommitted changes found, commit them
  before exiting(yes/no/cancel)? [cancel]:
  ```

  - When you enter `yes`, it saves the changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

  - When you enter **no**, it exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - When you enter **cancel**, it leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file, and remain within the configuration session.

Verifying the Frequency Synchronization Configuration

After performing the frequency synchronization configuration tasks, use this task to check for configuration errors and verify the configuration.

Procedure

Step 1 **show frequency synchronization configuration-errors**

Example:

```
RP/0/RP0:hostname# show frequency synchronization configuration-errors

  RP/0/RP0:ios#sh frequency synchronization configuration-errors
  Tue Aug  2 05:59:14.516 UTC
  Node 0/RP0:

==============
    interface TenGigE0/1/0/2 frequency synchronization
* Frequency synchronization is enabled on this interface, but isn't enabled globally.
RP/0/RP0:ios#
```

Displays any errors that are caused by inconsistencies between shared-plane (global) and local-plane (interface) configurations. There are two possible errors that can be displayed:

- The QL option configured on some interface does not match the global QL option. Under an interface (line interface), the QL option is specified using the **quality transmit** and **quality receive** commands. The value specified must match the value configured in the global **quality itu-t option** command, or match the default (option 1) if the global **quality itu-t option** command is not configured.

Once all the errors have been resolved, meaning there is no output from the command, continue to the next step.

Step 2 **show frequency synchronization interfaces brief**

Example:

```
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
```

Verifies the configuration. Note the following points:

- All line interface that have frequency synchronization configured are displayed.
- Sources that have been nominated as inputs (in other words, have **selection input** configured) have ‘S’ in the Flags column; sources that have not been nominated as inputs do not have ‘S’ displayed.

  Note Internal oscillators are always eligible as inputs.

- ‘>’ or ‘D’ is displayed in the flags field as appropriate.

If any of these items are not true, continue to the next step.

Step 3 **show frequency synchronization interfaces** *node-id*

Example:

```
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
```

Investigates issues within individual interfaces.

Step 4 **show processes fsyncmgr location** *node-id*

Example:

```
RP/0/RP0:hostname# show processes fsyncmgr location 0/0/CPU0

                  Job Id: 134
                     PID: 30202
         Executable path: /pkg/bin/fsyncmgr
              Instance #: 1
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 1
  Max. spawns per minute: 12
            Last started: Mon Mar  9 16:30:43 2009
           Process state: Run
           Package state: Normal
       Started on config: cfg/gl/freqsync/g/a/enable
                    core: MAINMEM
               Max. core: 0
               Placement: None
            startup_path: /pkg/startup/fsyncmgr.startup
                   Ready: 0.133s
        Process cpu time: 1730768.741 user, -133848.-361 kernel, 1596920.380 total
  --------------------------------------------------------------------------------
```

Verifies that the fsyncmgr process is running on the appropriate nodes.

Step 5 **show frequency synchronization clock-interfaces**

Example:

```
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
```

Step 6 **show frequency synchronization clock-interfaces brief**

Example:

```
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
```

Step 7 **show frequency synchronization clock-interfaces**

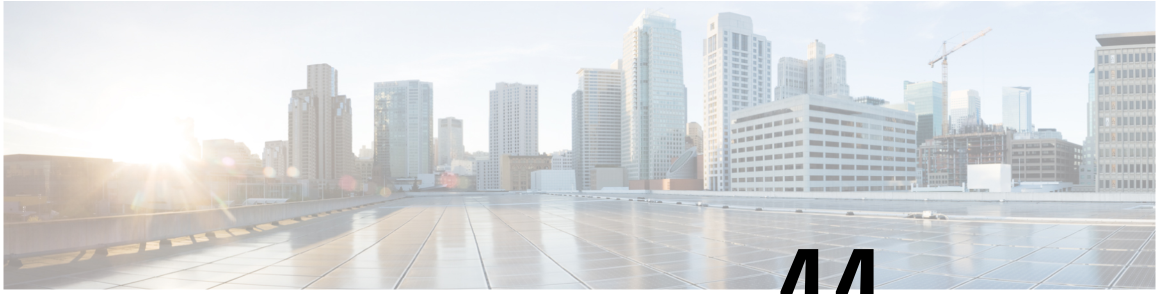
Example:

```
RP/0/RP0:hostname#show frequency synchronization clock-interfaces

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
```

Step 8 **show controllers timing controller clock**

Example:

```
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
```



CHAPTER 44

Configuring Point to Point Layer 2 Services

This chapter provides conceptual and configuration information for point-to-point Layer 2 (L2) connectivity on Cisco NCS 4000 Series routers.

Layer 2 Virtual Private Network Overview

Layer 2 Virtual Private Network (L2VPN) emulates the behavior of a LAN across an L2 switched, IP or MPLS-enabled IP network, allowing Ethernet devices to communicate with each other as they would when connected to a common LAN segment. Point-to-point L2 connections are vital when creating L2VPNs.

As Internet service providers (ISPs) look to replace their Frame Relay or Asynchronous Transfer Mode (ATM) infrastructures with an IP infrastructure, there is a need to provide standard methods of using an L2 switched, IP or MPLS-enabled IP infrastructure. These methods provide a serviceable L2 interface to customers; specifically, to provide virtual circuits between pairs of customer sites.

Building a L2VPN system requires coordination between the ISP and the customer. The ISP provides L2 connectivity; the customer builds a network using data link resources obtained from the ISP. In an L2VPN service, the ISP does not require information about a the customer's network topology, policies, routing information, point-to-point links, or network point-to-point links from other ISPs.

The ISP requires provider edge (PE) routers with these capabilities:

- Encapsulation of L2 protocol data units (PDU) into Layer 3 (L3) packets.
- Interconnection of any-to-any L2 transports.
- Emulation of L2 quality-of-service (QoS) over a packet switch network.
- Ease of configuration of the L2 service.
- Support for different types of tunneling mechanisms (MPLS TE, Flex LSP).
- L2VPN process databases include all information related to circuits and their connections.

Ethernet Virtual Circuit

Ethernet virtual circuits (EVCs) define a Layer 2 bridging architecture that supports Ethernet services. An EVC is defined by the Metro-Ethernet Forum (MEF) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual service pipe within the service provider network. On Cisco NCS 4000 Series Routers, the EVC is implemented as a pseudowire (PW). This section explains the basic rules for configuring EVC:

- **Enable L2 transport on an interface (l2transport command)** - A packet must be received on an interface configured with the l2transport keyword in order to be processed by the L2VPN feature. This interface can be a main interface, where the l2transport command is configured under the interface config mode, or a subinterface, where the l2transport keyword is configured after the sub interface number.

  Example:

  ```
  interface TenGigE0/0/0/2 l2transport
  ```

  ```
  interface TenGigE0/6/0/6.11 l2transport
  ```

- **Incoming Interface Matching (encapsulation command)** - This command is used to specify matching criteria. A longest match lookup determines the incoming interface of the packet. The longest match lookup checks these conditions in this order to match the incoming packet to a subinterface:
  - The incoming frame has two dot1q tags and matches a subinterface configured with the same two dot1q tags (802.1Q tunneling, or QinQ). This is the longest possible match.
  - The incoming frame has two dot1q tags and matches a subinterface configured with the same dot1q first tag and any for the second tag.
  - The incoming frame has one dot1q tag and matches a subinterface configured with the same dot1q tag and the exact keyword.
  - The incoming frame has one or more dot1q tags and matches a subinterface configured with one of the dot1q tags.
  - The incoming frame has no dot1q tags and matches a subinterface configured with the **encapsulation untagged** command.
  - The incoming frame fails to match any other subinterface, so it matches a subinterface configured with the **encapsulation default** command.

Note Assignment of incoming frames to a subinterface based on source MAC adress is not supported.

Following **examples** explain the use of the encapsulation command:

1. To match any tagged or untagged traffic that has not been matched by another subinterface with a longest match:

```
interface TenGigE0/1/0/3.1 l2transport
 encapsulation default
```

2. When there are multiple subinterfaces, run the longest match test on the incoming frame in order to determine the incoming interface:

```
interface TenGigE0/1/0/3.1 l2transport
 encapsulation default
!
interface TenGigE0/1/0/3.2 l2transport
 encapsulation dot1q 2
!
interface TenGigE0/1/0/3.3 l2transport
 encapsulation dot1q 2 second-dot1q 3
```

Note
- A QinQ frame with an outer VLAN tag 2 and an inner VLAN tag 3 could match the .1, .2, or .3 subinterfaces but it is assigned to the .3 subinterface because of the longest match rule. Two tags on .3 are longer than one tag on .2 and longer than no tags on .1.
- A QinQ frame with an outer VLAN tag 2 and an inner VLAN tag 4 is assigned to the .2 subinterface because encapsulation dot1q 2 can match dot1q frames with just the VLAN tag 2 but can also match QinQ frames with an outer tag 2. Refer to Example 3(the exact keyword) if you do not want to match the QinQ frames.
- A QinQ frame with an outer VLAN tag 3 matches the .1 subinterface.
- A dot1q frame with a VLAN tag 2 matches the .2 subinterface.
- A dot1q frame with a VLAN tag 3 matches the .1 subinterface.

3. To match a dot1q frame and not a QinQ frame, use the exact keyword:

```
interface TenGigE0/1/0/3.2 l2transport
 encapsulation dot1q 2 exact
```

Note This configuration does not match QinQ frames with an outer VLAN tag 2 because it matches only frames with exactly one VLAN tag.

4. Use the untagged keyword in order to match only untagged frames :

```
interface TenGigE0/1/0/3.1 l2transport
 encapsulation default
```

```
!
interface TenGigE0/1/0/3.2 l2transport
 encapsulation untagged
!
interface TenGigE0/1/0/3.3 l2transport
 encapsulation dot1q 3
```

Note

- Dot1q frames with a VLAN tag 3 or QinQ frames with an outer tag 3 match the .3 subinterfaces.
- All other dot1q or QinQ frames match the .1 subinterface.
- Frames without a VLAN tag match the .2 subinterface.

5. The "any" keyword can be used as wildcard:

```
interface TenGigE0/1/0/3.4 l2transport
 encapsulation dot1q 4 second-dot1q any
!
interface TenGigE0/1/0/3.5 l2transport
 encapsulation dot1q 4 second-dot1q 5
```

Note

- Both subinterfaces .4 and .5 could match QinQ frames with tags 4 and 5, but the frames are assigned to the .5 subinterfaces because it is more specific. This is the longest match rule.
- The "any" keyword option is not applicable with single VLAN dot1q or dot1ad. For example following is not supported:

  ```
  encapsulation dot1q any
  or
  encapsulation dot1ad any
  ```

6. Ranges of VLAN tags can be used:

```
interface TenGigE0/1/0/3.6 l2transport
 encapsulation dot1q 6-10
```

Note

- Per line card maximum 32 dot1q or dot1ad ranges (including both inner or outer range) can be configured.
- Multiple VLAN tag values or ranges are not supported.

7. The encapsulation dot1q second-dot1q command uses the Ethertype 0x8100 for the outer and inner tags because this is the Cisco method to encapsulate QinQ frames. According to IEEE, however, the Ethertype 0x8100 should be reserved for 802.1q frames with one VLAN tag, and an outer tag with Ethertype 0x88a8 should be used for QinQ frames. The outer tag with Ethertype 0x88a8 can be configured with the dot1ad keyword:

```
interface TenGigE0/1/0/3.12 l2transport
 encapsulation dot1ad 12 dot1q 100
```

8. In order to use the old Ethertype 0x9100 or 0x9200 for the QinQ outer tags, use the dot1q tunneling ethertype command under the main interface of the QinQ subinterface:

```
interface TenGigE0/1/0/3
 dot1q tunneling ethertype [0x9100|0x9200]
!
interface TenGigE0/1/0/3.13 l2transport
 encapsulation dot1q 13 second-dot1q 100
```

Note

- The outer tag has an Ethertype of 0x9100 or 0x9200, and the inner tag has the dot1q Ethertype 0x8100.
- Per interface only two Ethertype are supported. Whenever custom Ethertype are added for an interface, dot1ad configuration should not be present on that interface.

- **VLAN Manipulation (rewrite command)** - On a Cisco NCS 4000 Router that uses the EVC infrastructure, the default action is to preserve the VLAN tags on the incoming frame. But, the EVC infrastructure allows you to manipulate the tags with the rewrite command. Use the rewrite command to modify the default , so you can pop (remove), translate, or push (add) tags to the incoming VLAN tag stack.

Note Egress vlan filter is not supported, so when packet is egressing no egress vlan checks are performed.

Following **examples** explain the use of the rewrite command:

- The pop keyword lets you remove a QinQ tag from an incoming dot1q frame. This example removes the outer tag 13 of the incoming QinQ frame and forwards the frame with the dot1q tag 100 on top:

```
interface TenGigE0/1/0/3.13 l2transport
 encapsulation dot1q 13 second-dot1q 100
 rewrite ingress tag pop 1 symmetric
```

Note The behavior is always symmetric, which means that the outer tag 13 is popped in the ingress direction and pushed in the egress direction.

- The translate keyword lets you replace one or two incoming tags by one or two new tags:

```
RP/0/RP0:hostname(config-subif)#interface TenGigE0/1/0/3.3
   l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 3
RP/0/RP0:hostname(config-subif)#rewrite ingress tag translate ?
  1-to-1  Replace the outermost tag with another tag
  2-to-2  Replace the outermost two tags with two other tags
RP/0/RP0:hostname(config-subif)#rewrite ingress tag translate 1-to-1 ?
  dot1ad  Push a Dot1ad tag
  dot1q   Push a Dot1Q tag
RP/0/RP0:hostname(config-subif)#rewrite ingress tag translate 1-to-1
   dot1q 4
```

```
RP/0/RP0:hostname(config-subif)#show config
Building configuration...
!! IOS XR Configuration 4.3.0
interface TenGigE0/1/0/3.3 l2transport
 encapsulation dot1q 3
 rewrite ingress tag translate 1-to-1 dot1ad 20 symmetric
!
end
```

Note

- The symmetric keyword is added automatically because it is the only supported mode.
- translate 1-to-2 and 2-to-1 are not supported.
- translate 1-to-1 is not supported with dot1ad option.
- translate 2-to-2 is not supported for VPWS on NCS4K-2H10T-OP-KS card.

- The push keyword lets you add a QinQ tag to an incoming dot1q frame:

```
interface TenGigE0/1/0/3.4 l2transport
 encapsulation dot1q 4
 rewrite ingress tag push dot1q 100 symmetric
```

Note

- An outer QinQ tag 100 is added to the incoming frame with a dot1q tag 4. In the egress direction, the QinQ tag is popped.
- With encapsulation default, vlan push operations are not supported.
- Adding two tags with "push" is supported only with singled tagged or untagged encapsulation like for example:

  ```
  rewrite ingress tag push dot1q 20 second-dot1q 200 symmetric
  ```

- Adding two tags with "push" is not supported for VPWS on NCS4K-2H10T-OP-KS card.

Ethernet Wire Service

An Ethernet Wire Service is a service that emulates a point-to-point Ethernet segment. This is similar to Ethernet private line (EPL), a Layer 1 point-to-point service, except the provider edge operates at Layer 2 and typically runs over a Layer 2 network. The EWS encapsulates all frames that are received on a particular UNI and transports these frames to a single-egress UNI without reference to the contents contained within the frame. The operation of this service means that an EWS can be used with VLAN-tagged frames. The VLAN tags are transparent to the EWS (bridge protocol data units [BPDUs])-with some exceptions. These exceptions include IEEE 802.1x, IEEE 802.2ad, and IEEE 802.3x, because these frames have local significance and it benefits both the customer and the Service Provider to terminate them locally.

The customer side has these types:

- Untagged
- Single tagged
- Double tagged
- 802.1q
- 802.1ad

E-Line Service

E-Line service provides a point-to-point EVC between two UNIs. There are two types of E-Line services:

- Ethernet Private Line (EPL)
  - No service multiplexing allowed
  - Transparent
  - No coordination between customer and SP on VLAN ID map
- Ethernet Virtual Private Line (EVPL)
  - Allows service multiplexing
  - No need for full transparency of service frames

EPL and EVPL services are provided through:

- Layer 2 Local Switching, on page 623
- VPWS, on page 629

Layer 2 Local Switching

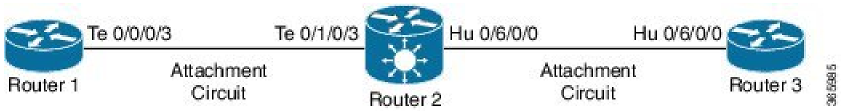
Local switching is a point-to-point circuit internal to a single Cisco NCS 4000 Series router, also known as local connect. Local switching allows you to switch L2 data between two interfaces of the same type, (for example, Ethernet to Ethernet) and on the same router. The interfaces can be on the same line card, or on two different line cards. During these types of switching, Layer 2 address is used instead of the Layer 3 address.

A local switching connection switches L2 traffic from one attachment circuit (AC) to the other. The two ports configured in a local switching connection are ACs with respect to that local connection.

Main Interface

The basic topology is a local cross connect between two main interfaces:

Figure 31:



Router2 takes all traffic received on Te 0/1/0/3 and forwards it to Hu 0/6/0/0 and vice versa.

While router1 and router3 appear to have a direct back-to-back cable in this topology, this is not the case because router2 is actually translating between the TenGigE and HundredGigE interfaces. Router2 can run features on these two interfaces.

A basic point-to-point cross connect is configured between two main interfaces that are configured as l2transport on router2:

```
 interface TenGigE0/1/0/3 l2transport
 !
!
interface HundredGigE0/6/0/0
 l2transport
 !
!
l2vpn
 xconnect group test
  p2p p2p1
   interface HundredGigE0/6/0/0
   interface TenGigE0/1/0/3
  !
```

On router1 and router3, the main interfaces are configured with IPv4 address:

```
RP/0/RP0:router1#sh run int Te 0/0/0/3
interface TenGigE0/0/0/3

 ipv4 address 10.1.1.1 255.255.255.0
!

RP/0/RP0:router1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/32 ms
```

Router1 sees router3 as a neighbor and can ping 10.1.1.2 (the interface address of router3) as if the two routers were directly connected.

Because there is no subinterface configured on router2, incoming frames with a VLAN tag are transported transparently when dot1q subinterfaces are configured on router1 and router3:

```
RP/0/RP0:router1#sh run int Te 0/0/0/3.2
interface TenGigE0/0/0/3.2
 ipv4 address 10.1.2.1 255.255.255.0
 dot1q vlan 2
!

RP/0/RP0:router1#ping 10.1.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
```

After 10,000 pings from router1 to router3, you can use the show interface and show l2vpn commands in order to ensure that ping requests received by router2 on one AC are forwarded on the other AC and that ping replies are handled the same way in reverse.

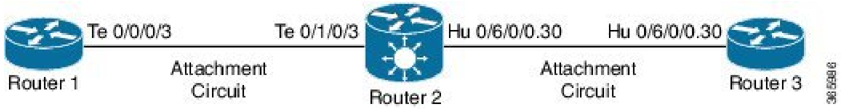
```
RP/0/RP0:router2#sh int Te 0/1/0/3
  TenGigE0/0/0/3 is up, line protocol is up
  Interface state transitions: 1
  Hardware is TenGigE, address is 0024.986c.63f1 (bia 0024.986c.63f1)
  Description: static lab connection to acdc 0/0/0/3 - dont change
  Layer 2 Transport Mode
  MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
```

```
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 1000Mb/s, SXFD, link type is force-up
  output flow control is off, input flow control is off
  loopback not set,
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters 00:01:07
  5 minute input rate 28000 bits/sec, 32 packets/sec
  5 minute output rate 28000 bits/sec, 32 packets/sec
     10006 packets input, 1140592 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 6 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10007 packets output, 1140832 bytes, 0 total output drops
     Output 0 broadcast packets, 7 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions


RP/0/RP0:router2#sh int Hu 0/6/0/0
HundredGigE0/6/0/0 is up, line protocol is up
  Interface state transitions: 3
  Hardware is HundredGigE, address is 0024.98ea.038b (bia 0024.98ea.038b)
  Layer 1 Transport Mode is LAN
  Description: static lab connection to putin 0/6/0/0 - dont change
  Layer 2 Transport Mode
  MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 10000Mb/s, LR, link type is force-up
  output flow control is off, input flow control is off
  loopback not set,
  Last input 00:00:00, output 00:00:06
  Last clearing of "show interface" counters 00:01:15
  5 minute input rate 27000 bits/sec, 30 packets/sec
  5 minute output rate 27000 bits/sec, 30 packets/sec
     10008 packets input, 1140908 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 8 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10006 packets output, 1140592 bytes, 0 total output drops
     Output 0 broadcast packets, 6 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions


RP/0/RP0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                Segment 1                    Segment 2
Group      Name    ST   Description         ST       Description         ST
---------------------   --------------------------   --------------------------
test       p2p1    UP   Hu0/6/0/0           UP       Te0/1/0/3           UP
--------------------------------------------------------------------------------
RP/0/RP0:router2#sh l2vpn xconnect group test det

Group test, XC p2p1, state is up; Interworking none
  AC: TenGigE0/0/0/3, state is up
    Type Ethernet
    MTU 1500; XC ID 0x1080001; interworking none
    Statistics:
      packets: received 10008, sent 10006
      bytes: received 1140908, sent 1140592
  AC: TenGigE0/1/0/3, state is up
    Type Ethernet
    MTU 1500; XC ID 0x1880003; interworking none
    Statistics:
      packets: received 10006, sent 10008
      bytes: received 1140592, sent 1140908

RP/0/RP0#sh l2vpn forwarding interface TenGigE 0/0/0/10 hardware ingress detail location
0/RP0
Local interface: TenGigE0/0/0/10, Xconnect id: 0x3a, Status: up
  Segment 1
    AC, TenGigE0/0/0/10, Ethernet port mode, status: Bound
    Statistics:
      packets: received 777274547, sent 731226431
      bytes: received 99047365649, sent 93179272680
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/1/0/0/100, Ethernet port mode, status: Bound

RP/0/RP0:router2#sh l2vpn forwarding interface Hu 0/6/0/0 hardware egress
   detail location 0/0
Local interface: HundredGigE0/6/0/0, Xconnect id: 0x1080001, Status: up
  Segment 1
    AC, HundredGigE0/6/0/0, Ethernet port mode, status: Bound
    Statistics:
      packets: received 10028, sent 10027
      bytes: received 1143016, sent 1142732
      packets dropped: PLU 0, tail 0
      bytes dropped: PLU 0, tail 0
  Segment 2
    AC, TenGigE0/1/0/3, Ethernet port mode, status: Bound

  Platform AC context:
  Egress AC: Local Switch, State: Bound
    Flags: Remote is Simple AC
  XID: 0x00000001, SHG: None
  Ingress uIDB: 0x0007, Egress uIDB: 0x0007, NP: 0, Port Learn Key: 0
  NP0
    Egress uIDB:
      Flags: L2, Status, Done
      Stats ptr: 0x000000
      VPLS SHG: None
      VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000
      UIDB IF Handle: 0x04000240, Search VLAN Vector: 0
      QOS ID: 0, QOS format: 0
    Xconnect ID: 0x00000001, NP: 0
      Type: AC, Remote type: AC
      Flags: Learn enable
      uIDB Index: 0x0007, LAG pointer: 0x0000
      Split Horizon Group: None
```

Subinterfaces and VLAN Manipulation

The basic topology is a local cross connect between a main interface and a sub interface:

Figure 32:



Following section describes how flexible rewrite capabilities give multiple ways to manipulate the VLAN :

1. Main Interface and Dot1q Subinterface

   In this example, the main interface is on one side, and the dot1q subinterface is on the other side:

   This is the main interface on router1:

```
RP/0/RP0:router1#sh run int te 0/0/0/3
interface TenGigE0/0/0/3
 description static lab connection to router2 0/1/0/3
 ipv4 address 10.1.1.1 255.255.255.0
!
```

   This is the dot1q subinterface on router2:

```
RP/0/RP0:router2#sh run int te 0/1/0/3
interface TenGigE0/1/0/3
 description static lab connection to router1 0/0/0/3
 l2transport

RP/0/RP0:router2#sh run int hu 0/6/0/0.30
interface HundredGigE0/6/0/0.30 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric

RP/0/RP0:router2#sh run l2vpn xconnect group test
l2vpn
 xconnect group test
  p2p p2p2
   interface HundredGigE0/6/0/0.30
   interface TenGigE0/1/0/3
```

   There is now an l2transport keyword in the subinterface name of HundredGigE0/6/0/0.30. Router3 sends dot1q frames with tag 2, which match the HundredGigE0/6/0/0.30 subinterface on router2.

   The incoming tag 2 is removed in the ingress direction by the rewrite ingress tag pop 1 symmetric command. Since the tag has been removed in the ingress direction on the HundredGigE0/6/0/0.30, the packets are sent untagged in the egress direction on TenGigE0/1/0/3.

   Router1 sends untagged frames, which match the main interface TenGigE0/1/0/3.

   There is no rewrite command on TenGigE0/1/0/3, so no tag is popped, pushed, or translated.

   When packets have to be forwarded out of HundredGigE0/6/0/0.30, the dot1q tag 2 is pushed due to the symmetric keyword in the rewrite ingress tag pop 1 command. The command pops one tag in the ingress direction but symmetrically pushes one tag in the egress direction. This is an example on router3:

```
RP/0/RP0:router3#sh run int hu 0/6/0/0.30
interface HundredGigE0/6/0/0.30
 ipv4 address 10.1.1.2 255.255.255.0
 encapsulation dot1q 2
```

   Monitor the subinterface counters with the same show interface and show l2vpn commands:

```
RP/0/RP0:router2#clear counters
Clear "show interface" counters on all interfaces [confirm]
RP/0/RP0:router2#clear l2vpn forwarding counters
```

```
RP/0/RP0:router2#
RP/0/RP0:router2#
RP/0/RP0:router2#sh int HundredGigE0/6/0/0.30
HundredGigE0/6/0/0.30 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 0024.98ea.038b
  Layer 2 Transport Mode
  MTU 1518 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
     reliability Unknown, txload Unknown, rxload Unknown
  Encapsulation 802.1Q Virtual LAN,
    Outer Match: Dot1Q VLAN 2
    Ethertype Any, MAC Match src any, dest any
  loopback not set,
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters 00:00:27
     1000 packets input, 122000 bytes
     0 input drops, 0 queue drops, 0 input errors
     1002 packets output, 122326 bytes
     0 output drops, 0 queue drops, 0 output errors


RP/0/RP0:router2#sh l2vpn xconnect detail

Group test, XC p2p2, state is up; Interworking none
  AC: HundredGigE0/6/0/0.30, state is up
    Type VLAN; Num Ranges: 1
    VLAN ranges: [2, 2]
    MTU 1500; XC ID 0x1080001; interworking none
    Statistics:
      packets: received 1001, sent 1002
      bytes: received 118080, sent 118318
      drops: illegal VLAN 0, illegal length 0
  AC: TenGigE0/1/0/3, state is up
    Type Ethernet
    MTU 1500; XC ID 0x1880003; interworking none
    Statistics:
      packets: received 1002, sent 1001
      bytes: received 114310, sent 114076
```

As expected, the number of packets received on HundredGigE0/6/0/0.30 matches the number of packets sent on TenGigE0/1/0/3 and vice versa.

2. Subinterface with Encapsulation

   Instead of the main interface on TenGigE0/1/0/3, you can use a subinterface with encapsulation default in order to catch all frames or with encapsulation untagged in order to match only untagged frames:

```
RP/0/RP0:router2#sh run interface TenGigE0/1/0/3.1
interface TenGigE0/1/0/3.1 l2transport
 encapsulation untagged

RP/0/RP0:router2#sh run int HundredGigE0/6/0/0.30
interface HundredGigE0/6/0/0.30 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric

RP/0/RP0:router2#sh run l2vpn xconnect group test
l2vpn
 xconnect group test
  p2p p2p3
   interface HundredGigE0/6/0/0.30
   interface TenGigE0/1/0/3.1
```

3. Ingress Direction on TenGigE0/1/0/3.1

Rather than pop tag 2 in the ingress direction on HundredGigE0/6/0/0.30, you can push tag 2 in the ingress direction on TenGigE0/1/0/3.1 and not do anything on HundredGigE0/6/0/0.30:

```
RP/0/RP0:router2#sh run int  HundredGigE0/6/0/0.30
interface HundredGigE0/6/0/0.30 l2transport
 encapsulation dot1q 2

RP/0/RP0:router2#sh run interface TenGigE0/1/0/3.1
interface TenGigE0/1/0/3.1 l2transport
 encapsulation untagged
 rewrite ingress tag push dot1q 2 symmetric

RP/0/RP0:router2#sh run int HundredGigE0/6/0/0.30
interface HundredGigE0/6/0/0.30 l2transport
 encapsulation dot1q 2

RP/0/RP0:router2#sh run l2vpn xconnect group test
l2vpn
 xconnect group test
  p2p p2p3
   interface HundredGigE0/6/0/0.30
   interface TenGigE0/1/0/3.1
```

Thus, you can see that the EVC model with the encapsulation and rewrite commands gives you great flexibility to match and manipulate VLAN tags.

Limitations :

- Pseudo wire redundancy is not supported

VPWS

Table 48: Feature History

Feature Name	Release Information	Feature Description
Support for Flow Label Load Balancing	Cisco IOS XR Release 6.5.31	Prior to R6.5.31, Flow-Aware Transport Pseudowire (FAT-PW) load balancing is supported on the Link Aggregation Group (LAG) NNI interface with insertion up to three labels. From R6.5.31 onwards, FAT-PW load balancing is supported on the LAG NNI interface with insertion up to five labels. This enhancement allows the flow-aware traffic to be optimally load balanced among all the links on the LAG AC interfaces.

Virtual Private Wire Services (VPWS), also known as Ethernet-over-MPLS (EoMPLS), allow two L2VPN Provider Edge (PE) devices to tunnel the Ethernet traffic through an MPLS-enabled L3 core and encapsulates Ethernet protocol data units (PDUs) inside MPLS packets (using label stacking) to forward them across the MPLS cloud. The two L2VPN PEs are typically connected at two different sites with an MPLS core between them. The two attachment circuits (ACs)connected at each L2VPN PE are linked by a pseudo wire (PW) over the MPLS network, which is the MPLS PW. The pseudo wire is a virtual point-to-point circuit and is always a type 5 virtual connection (VC). Type 4 VCs and Control Word (CW) are not supported.

For more information on pseudo wire types, see Type 5 Pseudo Wires, on page 634. The number of PWs supported on NCS4K-4H-OPW-QC2 and NCS4K-2H10T-OP-KS cards is 1000.

The two PEs establish an MPLS LDP targeted session between themselves so they can establish and control the status of the PW. An MPLS LDP targeted session is a label distribution session between routers that are not directly connected. When you create an MPLS traffic engineering tunnel interface, you need to establish a label distribution session between the tunnel headend and the tailend routers.The MPLS LDP targeted session is established over:

- Flex LSP. For more information
- MPLS TE.

EoMPLS features are described in this subsection:

- Ethernet Port Mode, on page 633

Pseudo wire redundancy is not supported.

VPWS Scale

The following table displays the scale numbers for VPWS:

Line Card	Scale
NCS4K-2H10T-OP-KS line card	1000
NCS4K-4H-OPW-QC2 line card	1000

Sytem	Scale
Node with NCS4K-2H10T-OP-KS and NCS4K-4H-OPW-QC2 line cards	4000
Node with NCS4K-4H-OPW-QC2 line cards	4000

FAT Pseudo Wires

In a VPWS network, the flow aware transport (FAT) of pseudowires can be used for load balancing traffic across LDP-signaled pseudowires. A flow label is a unique identifier to distinguish a flow within the pseudowire. These flow labels enable load balancing of MPLS packets across equal cost multipath (ECMP) paths or link aggregation groups (LAGs).When the pseudowire is configured to use the flow labels for load balancing, packets arriving at the ingress PE node are processed. A flow label is inserted for each packet between the VC label and control word.The flow label is derived from the payload of the inbound packet using a hash-key algorithm. The ingress router pushes the flow label to the label stack of the packet. At the egress PE node, hashing is performed using the terminated headers, including the flow label to balance traffic across LAG members.

To balance the load based on flow labels, use the **load-balancing flow-label**command in the l2vpn pseudowire class mpls configuration submode.

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 Release 6.5.31 onwards, FAT-PW load balancing is supported for LAG NNI interface with insertion upto five labels.

Pseudowire Call Admission Control (CAC)

You can use the Pseudowire Call Admission Control (PW CAC) process to check for bandwidth constraints and ensure that after the path is signaled, the links (pseudowires participating in the bidirectional LSP association have the required bandwidth. Only pseudowires with sufficient bandwidth are admitted in the bidirectional LSP association process. The PW CAC feature works only when the PW is configured with a L2VPN preferred path tunnel.

You can configure bandwidth allocation and call admission control on layer 2 circuits. When you configure bandwidth on a layer 2 circuit, attempts to establish a bidirectional LSP is preceded by a check of the available bandwidth on the network. The available bandwidth is compared to the bandwidth requested by the LSP. If there is insufficient bandwidth, the circuit is not established.

To verify if the requested bandwidth has been allocated and whether the PW is up, use the **l2vpn xconnect detail** command. The following examples display the verification output.

Example:1

Requested bandwidth is available. In this scenario, the PW is up.

```
Group VPWS, XC p1, state is up; Interworking none
  AC: FortyGigE0/9/0/9.1, state is up
    Type VLAN; Num Ranges: 0
    MTU 9202; XC ID 0x1; interworking none
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
      drops: illegal VLAN 0, illegal length 0
  PW: neighbor 3.3.3.3, PW ID 1, state is up ( established )
    PW class vpws1, XC ID 0xc0000001
    Encapsulation MPLS, protocol LDP
    Source address 1.1.1.1
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
    Preferred path tunnel TE 1, fallback enabled
    Required BW = 1000 Admited BW = 1000
    PW Status TLV in use
      MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        24006                          24000
      Group ID     0x800164c                      0x80002f4
      Interface    FortyGigE0/9/0/9.1             FortyGigE0/8/0/9.1
      MTU          9202                           9202
      Control word disabled                       disabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x6                            0x6
                   (router alert label)           (router alert label)
                   (TTL expiry)                   (TTL expiry)
      ------------ ------------------------------ -----------------------------
    Incoming Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
    Outgoing Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
    MIB cpwVcIndex: 3221225473
    Create time: 21/03/2017 13:09:36 (17:32:46 ago)
    Last time status changed: 22/03/2017 06:29:19 (00:13:03 ago)
    Last time PW went down: 21/03/2017 15:31:24 (15:10:58 ago)
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
```

Example 2:

Requested bandwidth is not available. In this scenario the PW is down.

```
Group VPWS, XC p1, state is down; Interworking none
  AC: FortyGigE0/9/0/9.1, state is up
    Type VLAN; Num Ranges: 0
    MTU 9202; XC ID 0x256; interworking none
    Statistics:
      packets: received 18016128, sent 97172
      bytes: received 2288436524, sent 444659512
      drops: illegal VLAN 0, illegal length 0
  PW: neighbor 3.3.3.3, PW ID 1, state is down ( all ready )
    PW class vpws1, XC ID 0xc0000001
    Encapsulation MPLS, protocol LDP
    Source address 1.1.1.1
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
    Preferred path tunnel TE 1, fallback enabled
    Required BW = 475000 Admited BW = 0
    PW Status TLV in use
      MPLS         Local                          Remote
      ------------ ------------------------------ -----------------------------
      Label        24007                          24001
      Group ID     0x8000d7c                      0x80018fc
      Interface    FortyGigE0/9/0/9.1             FortyGigE0/8/0/9.1
      MTU          9202                           9202
      Control word disabled                       disabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x6                            0x6
                   (router alert label)           (router alert label)
                   (TTL expiry)                   (TTL expiry)
      ------------ ------------------------------ -----------------------------
    Incoming Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
    Outgoing Status (PW Status TLV):
      Status code: 0x10 (PW Down) in Notification message
    MIB cpwVcIndex: 3221225473
    Create time: 25/03/2017 19:09:14 (1d14h ago)
    Last time status changed: 27/03/2017 09:23:23 (00:00:03 ago)
    Last time PW went down: 27/03/2017 09:23:23 (00:00:03 ago)
    Statistics:
      packets: received 97172, sent 18016128
      bytes: received 444659512, sent 2288436524
```

VPWS and PW Scale Details

Scale details for VPWS and PW:

Table 49: Supported LSPs for VPWS and PW

VPWS over physical interface	8000 LSPs
VPWS over bundle interface	1000 LSPs

MPLS Label Distribution Protocol (LDP) Overview

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) provides the means for peer label switch routers (LSRs) to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

MPLS LDP enables one LSR to inform another LSR of the label bindings it has made. Once a pair of routers communicate the LDP parameters, they establish a label-switched path (LSP). MPLS LDP enables LSRs to distribute labels along normally routed paths to support MPLS forwarding. This method of label distribution is also called hop-by-hop forwarding. With IP forwarding, when a packet arrives at a router the router looks at the destination address in the IP header, performs a route lookup, and forwards the packet to the next hop. With MPLS forwarding, when a packet arrives at a router the router looks at the incoming label, looks up the label in a table, and then forwards the packet to the next hop. MPLS LDP is useful for applications that require hop-by-hop forwarding, such as MPLS VPNs.

When you enable MPLS LDP, the LSRs send out messages to try to find other LSRs with which they can create LDP sessions. LDP sessions can be Directly Connected MPLS LDP Sessions or Nondirectly Connected MPLS **LDP Sessions**.

In a **Directly Connected MPLS LDP Session**, LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends out LDP link Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet (multicast). A neighboring LSR may respond to the link Hello message, allowing the two routers to establish an LDP session. This is called basic discovery.

In a **Nondirectly Connected MPLS LDP Session**, LSR is more than one hop from its neighbor, it is non-directly connected to its neighbor. For these non-directly connected neighbors, the LSR sends out a targeted Hello message as a UDP packet, but as a unicast message specifically addressed to that LSR. The nondirectly connected LSR responds to the Hello message and the two routers begin to establish an LDP session. This is called extended discovery. **An MPLS LDP targeted session** is a label distribution session between routers that are not directly connected. When you create an MPLS traffic engineering tunnel interface, you need to establish a label distribution session between the tunnel head-end and the tail-end routers. You establish nondirectly connected MPLS LDP sessions by enabling the transmission of targeted Hello messages.

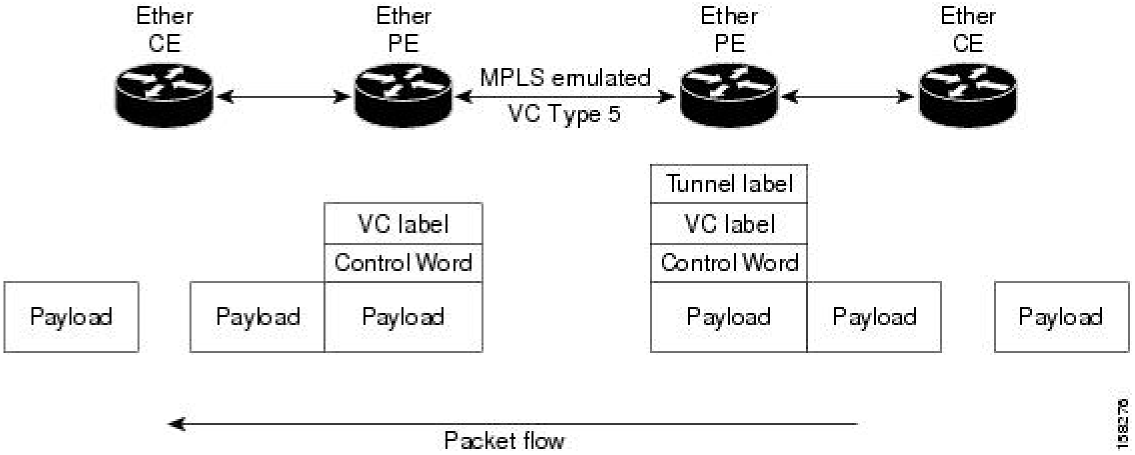
Note Only MPLS LDP targeted sessions are supported.

Ethernet Port Mode

In Ethernet port mode, both ends of a pseudowire are connected to Ethernet ports. In this mode, the port is tunneled over the pseudowire or, using local switching (also known as an attachment circuit-to-attachment circuit cross-connect) switches packets or frames from one attachment circuit (AC) to another AC attached to the same PE node.

The following figure provides an example of Ethernet port mode.

Figure 33: Ethernet Port Mode Packet Flow



Type 5 Pseudo Wires

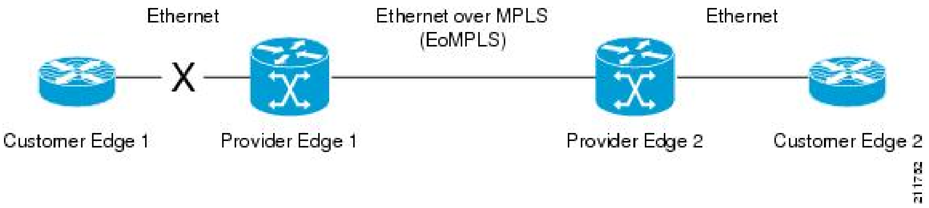
A type 5 PW is known as an Ethernet port-based PW. The ingress PE transports frames received on a main interface or after the subinterface tags have been removed when the packet is received on a subinterface. There is no requirement to send a tagged frame over a type 5 PW, and no dummy tag is added by the EVC-based platforms. The EVC-based platforms have the ability to manipulate the VLAN tags received on the incoming frame with the rewrite command. The results of that VLAN manipulation are transported over the type 5 PW, whether tagged or untagged.

Ethernet Remote Port Shutdown

Ethernet remote port shutdown provides a mechanism for the detection and propagation of remote link failure for port mode EoMPLS on a Cisco NCS 4000 router line card. This lets a service provider edge router on the local end of an Ethernet-over-MPLS (EoMPLS) pseudowire detect a cross-connect or remote link failure and cause the shutdown of the Ethernet port on the local customer edge router. Shutting down the Ethernet port on the local customer edge router prevents or mitigates a condition where that router would otherwise lose data by forwarding traffic continuously to the failed remote link, especially if the link was configured as a static IP route .

The figure below illustrates a condition in an EoMPLS WAN, with a down Layer 2 tunnel link between a CE router (Customer Edge 1) and the PE router (Provider Edge 1). A CE router on the far side of the Layer 2 tunnel (Customer Edge 2), continues to forward traffic to Customer Edge 1 through the L2 tunnel.

Figure 34: Remote Link Outage in EoMPLS Wide Area Network



Previous to this feature, the Provider Edge 2 router could not detect a failed remote link. Traffic forwarded from Customer Edge 2 to Customer Edge 1 would be lost until routing or spanning tree protocols detected the down remote link. If the link was configured with static routing, the remote link outage would be even more difficult to detect.

With this feature, the Provider Edge 2 router detects the remote link failure and causes a shutdown of the local Customer Edge 2 Ethernet port. When the remote L2 tunnel link is restored, the local interface is automatically restored as well. The possibility of data loss is thus diminished.

With reference to the figure above, the Remote Ethernet Shutdown sequence is generally described as follows:

1. The remote link between Customer Edge 1 and Provider Edge 1 fails.
2. Provider Edge 2 detects the remote link failure and disables the transmit laser on the line card interface connected to Customer Edge 2.
3. An RX_LOS error alarm is received by Customer Edge 2 causing Customer Edge 2 to bring down the interface
4. Provider Edge 2 maintains its interface with Customer Edge 2 in an up state.
5. When the remote link and EoMPLS connection is restored, the Provider Edge 2 router enables the transmit laser.
6. The Customer Edge 2 router brings up its interface

To enable this functionality, use the**l2transport propagate** command .

Example

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
```

VPWS - Sample Configuration Workflow

Complete these configurations on the provider edge routers to enable VPWS.

Topology

```
--(Te0/3/0/11)-[PE1]-(Hu0/14/0/0)-----(Hu0/5/0/0)-[PE2]-(Te0/5/0/9)--
```

where:

- TenGigE0/3/0/11 and TenGigE0/5/0/9 are the access or customer interfaces
- HundredGigE0/14/0/0 and HundredGigE0/5/0/0 are the core interfaces
- PE1 and PE2 are the two L2VPN provider edge (PE) routers. The two PEs are typically connected at two different sites with an MPLS core between them. The attachment circuits (ACs)connected at each L2VPN PE are linked by a pseudowire (PW) over the MPLS network.

Task 1: Bring up the controllers in lan-phy or packet termination mode.

Sample Configuration on PE1	Sample Configuration on PE2
! controller Optics0/3/0/11 port-mode Ethernet framing packet rate 10GE no shut ! controller Optics0/14/0/0 port-mode Ethernet framing packet rate 100GE no shut !	! controller Optics0/5/0/9 port-mode Ethernet framing packet rate 10GE no shut ! controller Optics0/5/0/0 port-mode Ethernet framing packet rate 100GE no shut !

Task 2: Bring up the access and core interfaces.

Sample Configuration on PE1	Sample Configuration on PE2
Access interface: interface TenGigE0/3/0/11 ! interface TenGigE0/3/0/11.1 l2transport encapsulation dot1q 1 no shut ! interface TenGigE0/3/0/11.2 l2transport encapsulation dot1q 2 no shut ! Core interface: interface HundredGigE0/14/0/0 ipv4 address 1.76.1.1 255.255.255.0 ! !	Access interface: interface TenGigE0/5/0/9 ! interface TenGigE0/5/0/9.1 l2transport encapsulation dot1q 1 no shut ! interface TenGigE0/5/0/9.2 l2transport encapsulation dot1q 2 no shut ! Core interface: interface HundredGigE0/5/0/0 ipv4 address 1.76.1.2 255.255.255.0 ! !
Details: Two access interfaces are brought up so that two pseudowires can be created.	

Task 3: Define loopback address.

Sample Configuration on PE1	Sample Configuration on PE2

`!`
`interface Loopback0`
` ipv4 address 1.1.1.1 255.255.255.255`
`!`
	`!`
	`interface Loopback0`
	` ipv4 address 3.3.3.3 255.255.255.255`
	`!`

Task 4: Configure the routing process using OSPF or ISIS on the core interface.

Sample Configuration on PE1	Sample Configuration on PE2

`router ospf 100`
`router-id 1.1.1.1`
`nsf`
`nsr`
` area 0`
` mpls traffic-eng`
` interface Loopback0`
`  !`
`  interface HundredGigE0/14/0/0`
`  !`
` !`
` mpls traffic-eng router-id Loopback0`
` !`
	`router ospf 100`
	`router-id 3.3.3.3`
	`nsf`
	`nsr`
	` area 0`
	` mpls traffic-eng`
	` interface Loopback0`
	`  !`
	`  interface HundredGigE0/5/0/0`
	`  !`
	` !`
	` mpls traffic-eng router-id Loopback0`
	` !`

Details: The sample configuration uses OSPF.	

Task 5: Configure MPLS traffic engineering on the core interface.

Sample Configuration on PE1	Sample Configuration on PE2

`mpls traffic-eng`
`interface HundredGigE0/14/0/0`
` !`
` fault-oam`
` !`
	`mpls traffic-eng`
	`interface HundredGigE0/5/0/0`
	` !`
	` fault-oam`
	` !`

Task 6: Configure RSVP on the core interface.

Sample Configuration on PE1	Sample Configuration on PE2

`rsvp`
`interface HundredGigE0/14/0/0`
`bandwidth 100`
` !`
`!`
	`rsvp`
	`interface HundredGigE0/5/0/0`
	`bandwidth 100`
	` !`
	`!`

Task 7: Configure MPLS OAM for MPLS pseudowires to work on the core interfaces.

Sample Configuration on PE1	Sample Configuration on PE2

`!`
`mpls oam`
`!`
	`!`
	`mpls oam`
	`!`

Task 8: Configure the tunnel interface. It can be a MPLS-TE or Flex-LSP tunnel.

Sample Configuration on PE1	Sample Configuration on PE2

Sample Configuration on PE1	Sample Configuration on PE2
MPLS TE tunnel:	MPLS TE tunnel:
`interface tunnel-te1`	`interface tunnel-te1`
`ipv4 unnumbered Loopback0`	`ipv4 unnumbered Loopback0`
`signalled-bandwidth 1`	`signalled-bandwidth 1`
`destination 3.3.3.3`	`destination 1.1.1.1`
`path-selection`	`path-selection`
`metric te`	`metric te`
`bandwidth 50000`	`bandwidth 50000`
`!`	`!`
` path-option 1 dynamic`	` path-option 1 dynamic`
`!`	`!`
Flex-LSP tunnel with BFD:	Flex-LSP tunnel with BFD:
`interface tunnel-te2`	`interface tunnel-te2`
`ipv4 unnumbered Loopback0`	`ipv4 unnumbered Loopback0`
`bfd`	`bfd`
` encap-mode gal`	` encap-mode gal`
` multiplier 3`	` multiplier 3`
` fast-detect`	` fast-detect`
` minimum-interval 100`	` minimum-interval 100`
` !`	` !`
` signalled-bandwidth 1`	` signalled-bandwidth 1`
` destination 3.3.3.3`	` destination 1.1.1.1`
` bidirectional`	` bidirectional`
` association id 86 source-address 192.0.0.0`	` association id 86 source-address 192.0.0.0`
` association type co-routed`	` association type co-routed`
`   fault-oam`	`   fault-oam`
`  !`	`  !`
` !`	` !`
`path-selection`	`path-selection`
`  metric te`	`  metric te`

Sample Configuration on PE1	Sample Configuration on PE2
bandwidth 50000 ! path-option 1 dynamic !	bandwidth 50000 ! path-option 1 dynamic !
Details: This is the tunnel bandwidth configuration that is required for VPWS CAC to work. The pseudowire requested bandwidth must be within the tunnel bandwidth value.	

Task 9: Setup interfaces running LDP:

Sample Configuration on PE1	Sample Configuration on PE2
mpls ldp nsr log neighbor nsr graceful-restart ! graceful-restart reconnect-timeout 169 graceful-restart forwarding-state-holdtime 180 discovery targeted-hello holdtime 180 targeted-hello interval 20 ! router-id 1.1.1.1 session protection address-family ipv4 discovery targeted-hello accept ! !	mpls ldp nsr log neighbor nsr graceful-restart ! graceful-restart reconnect-timeout 169 graceful-restart forwarding-state-holdtime 180 discovery targeted-hello holdtime 180 targeted-hello interval 20 ! router-id 3.3.3.3 session protection address-family ipv4 discovery targeted-hello accept ! !
Details: The two PEs establish a targeted MPLS LDP session between themselves so they can establish and control the status of the pseudowire. The targeted MPLS LDP session is established over MPLS-TE or Flex LSP.	

Task 10: Configure VPWS static and dynamic pseudowires.

Sample Configuration on PE1	Sample Configuration on PE2

Pseudowire 1 (vpws-pw-1) uses MPLS-TE tunnel (tunnel-te 1):
`l2vpn`
`pw-class vpws-pw-1`
`encapsulation mpls`
`protocol ldp`
`ipv4 source 1.1.1.1`
`preferred-path interface tunnel-te 1`
` !`
	Pseudowire 1 (vpws-pw-1) uses MPLS-TE tunnel (tunnel-te 1):
	`l2vpn`
	`pw-class vpws-pw-1`
	`encapsulation mpls`
	`protocol ldp`
	`ipv4 source 3.3.3.3`
	`preferred-path interface tunnel-te 1`
	` !`

Pseudowire 2 (vpws-pw-2) uses Flex-LSP tunnel (tunnel-te 2):
`!`
` pw-class vpws-pw-2`
` encapsulation mpls`
` protocol ldp`
` ipv4 source 1.1.1.1`
` preferred-path interface tunnel-te 2`
`!`
	Pseudowire 2 (vpws-pw-2) uses Flex-LSP tunnel (tunnel-te 2):
	`!`
	` pw-class vpws-pw-2`
	` encapsulation mpls`
	` protocol ldp`
	` ipv4 source 3.3.3.3`
	` preferred-path interface tunnel-te 2`
	`!`

Configure pseudowire 1 (vpws-pw-1) as dynamic:
`!`
` xconnect group vpws`
` p2p pw1`
` interface TenGigE0/3/0/11.1`
` neighbor ipv4 3.3.3.3 pw-id 1`
` bandwidth 1000`
` pw-class vpws-pw-1`
` !`
	Configure pseudowire 1 (vpws-pw-1) as dynamic:
	`!`
	` xconnect group vpws`
	` p2p pw1`
	` interface TenGigE0/5/0/9.1`
	` neighbor ipv4 1.1.1.1 pw-id 1`
	` bandwidth 1000`
	` pw-class vpws-pw-1`
	` !`

Sample Configuration on PE1	Sample Configuration on PE2
Configure pseudowire 2(vpws-pw-2) as static: ! p2p pw2 interface TenGigE0/3/0/11.2 neighbor ipv4 3.3.3.3 pw-id 2 mpls static label local 100 remote 200 bandwidth 1000 pw-class vpws-pw-2 ! !	Configure pseudowire 2(vpws-pw-2) as static: ! p2p pw2 interface TenGigE0/5/0/9.2 neighbor ipv4 1.1.1.1 pw-id 2 mpls static label local 100 remote 200 bandwidth 1000 pw-class vpws-pw-2 ! !
Details: The bandwidth command is used to allocate bandwidth to the pseudowire for VPWS CAC to function .	

Task 11: Configure flow label load balancing

Sample Configuration on PE1	Sample Configuration on PE2

l2vpn
 pw-class test5
  encapsulation mpls
   protocol ldp
   load-balancing
    flow-label both
   !
   preferred-path interface tunnel-te 5
  !
 !
!
 xconnect group vpws
 p2p g5
  interface TenGigE0/1/0/11
   neighbor ipv4 2.2.2.2 pw-id 5
   pw-class test5
   !
  !
	l2vpn
	 pw-class test5
	  encapsulation mpls
	   protocol ldp
	   load-balancing
	    flow-label both
	   !
	   preferred-path interface tunnel-te 5
	  !
	 !
	!
	 xconnect group vpws
	 p2p g5
	   interface Bundle-Ether100
	    neighbor ipv4 202.202.202.202 pw-id 5
	    pw-class test5
	    !
	   !
	  !
	 !

High Availability

L2VPN uses control planes in both route processors and line cards, as well as forwarding plane elements in the line cards.

The availability of L2VPN meets these requirements:

- A control plane failure in either the route processor or the line card will not affect the circuit forwarding path.
- The router processor control plane supports failover without affecting the line card control and forwarding planes.
- L2VPN integrates with existing targeted Label Distribution Protocol (LDP) graceful restart mechanism.

Preferred Tunnel Path

Preferred tunnel path functionality lets you map pseudowires to specific traffic-engineering tunnels. Attachment circuits are cross-connected to specific MPLS traffic engineering tunnel interfaces instead of remote PE router IP addresses (reachable using IGP or LDP). Using preferred tunnel path, it is always assumed that the traffic engineering tunnel that transports the L2 traffic runs between the two PE routers (that is, its head starts at the imposition PE router and its tail terminates on the disposition PE router). Preferred tunnel path configuration applies only to MPLS encapsulation.

Understanding L2VPN Nonstop Routing

The L2VPN Nonstop Routing (NSR) feature avoids label distribution path (LDP) sessions from flapping on events such as process failures (crash) and route processor failover (RP FO). NSR on process failure (crash) is supported by performing RP FO, if you have enabled NSR using NSR process failure switchover.

NSR enables the router (where failure has occurred) to maintain the control plane states without a graceful restart (GR). NSR, by definition, does not require any protocol extension and typically uses Stateful Switch Over (SSO) to maintain it's control plane states.

Configuring L2VPN Interface or Connection for L2VPN

Perform this task to configure an interface or a connection for L2VPN.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** *type interface-path-id* **l2transport**

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/6.11 l2transport
```

Enters interface configuration mode, configures an interface and enables L2 transport on the interface.

Step 3 **exit**

Example:

```
RP/0/RP0:hostname(config-if-l2)# exit
```

Exits the configuration mode.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE0/6/0/6.11
```

Enters interface configuration mode and configures an interface.

Step 5 **end or commit**

Example:

```
RP/0/RP0:hostname(config-if)# end
or
RP/0/RP0:hostname(config-if)# commit
```

- When you issue the end command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 6 **show interface** *type interface-id*

Example:

```
RP/0/RP0:hostname# show interface TenGigE0/6/0/6.11
```

(Optional) Displays the configuration settings you committed for the interface.

Configuring Local Switching

Perform this task to configure local switching.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **l2vpn**

Example:

```
RP/0/RP0:hostname# l2vpn
```

Enters L2VPN configuration mode.

Step 3 **xconnect group** *group-name*

Example:

```
RP/0/RP0:hostname(config-l2vpn)# xconnect group grp_1
```

Enters the name of the cross-connect group.

Step 4 **p2p** *xconnect-name*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc)# p2p vlan1
```

Enters a name for the point-to-point cross-connect.

Step 5 **interface** *interface-path-id*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface TenGigE0/6/0/2.10
```

Specifies the interface type ID. The choices are:

- TenGigE: TenGigabit Ethernet/IEEE 802.3 interfaces.
- HundredGigE: Hundred Gigabit Ethernet/IEEE 802.3 interfaces.
- CEM: Circuit Emulation interface.

Step 6 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface HundredGigE0/3/0/0.30
```

Specifies the interface type ID. The choices are:

- TenGigE: TenGigabit Ethernet/IEEE 802.3 interfaces.
- HundredGigE: Hundred Gigabit Ethernet/IEEE 802.3 interfaces.

Step 7 **end or commit**

Example:

```
RP/0/RP0:hostname(config-if)# end
or
RP/0/RSP0/CPU0:router(config-if)# commit
```

- When you issue the end command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Static Point to Point Cross-Connect

Perform this task to configure static point-to-point cross-connects.

Please consider this information about cross-connects when you configure static point-to-point cross-connects:

- An cross-connect is uniquely identified with the pair; the cross-connect name must be unique within a group.
- A segment (an attachment circuit or pseudowire) is unique and can belong only to a single cross-connect.
- A static VC local label is globally unique and can be used in one pseudowire only
- No more than 16,000 cross-connects can be configured per router.

Note Static pseudowire connections do not use LDP for signaling.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **l2vpn**

Example:

```
RP/0/RP0:hostname(config)# l2vpn
```

Enters L2VPN configuration mode.

Step 3 **xconnect group** *group-name*

Example:

```
RP/0/RP0:hostname(config-l2vpn)# xconnect group grp_1
```

Enters the name of the cross-connect group.

Step 4 **p2p** *xconnect-name*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc)# p2p vlan1
```

Enters a name for the point-to-point cross-connect.

Step 5 **interface** *interface-path-id*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface TenGigE0/6/0/2.10
```

Specifies the interface type and instance.

Step 6 **neighbor** A.B.C.D **pw-id** pseudowire-id

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor 10.2.2.2 pw-id 2000
```

Configures the pseudowire segment for the cross-connect.

Use the A.B.C.D argument to specify the IP address of the cross-connect peer.

Note A.B.C.D can be a recursive or non-recursive prefix.

Optionally, you can disable the control word or set the transport-type to Ethernet or VLAN.

Step 7 **mpls static label local** *value* **remote** *value*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# mpls static label local 699 remote 890
```

Configures local and remote label ID values.

Step 8 **end or commit**

Example:

```
RP/0/RP0:hostname(config-if)# end
or
RP/0/RP0:hostname(config-if)# commit
```

- When you issue the end command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Dynamic Point to Point Cross-Connect

Perform this task to configure dynamic point-to-point cross-connects.

Note For dynamic cross-connects, LDP must be up and running.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **l2vpn**

Example:

```
RP/0/RP0:hostname(config)# l2vpn
```

Enters L2VPN configuration mode.

Step 3 **xconnect group** *group-name*

Example:

```
RP/0/RP0:hostname(config-l2vpn)# xconnect group grp_1
```

Enters the name of the cross-connect group.

Step 4 **p2p** *xconnect-name*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc)# p2p vlan1
```

Enters a name for the point-to-point cross-connect.

Step 5 **interface** *interface-path-id*

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface TenGigE0/6/0/2.10
```

Specifies the interface type ID. The choices are:

- TenGigE: TenGigabit Ethernet/IEEE 802.3 interfaces.
- HundredGigE: Hundred Gigabit Ethernet/IEEE 802.3 interfaces.
- CEM: Circuit Emulation interface.

Step 6 **neighbor** A.B.C.D **pw-id** pseudowire-id

Example:

```
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor 10.2.2.2 pw-id 2000
```

Configures the pseudowire segment for the cross-connect.

Optionally, you can disable the control word or set the transport-type to Ethernet or VLAN.

Step 7 **end or commit**

Example:

```
RP/0/RP0:hostname(config-if)# end
or
RP/0/RP0:hostname(config-if)# commit
```

- When you issue the end command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring L2VPN Quality of Service

This section describes how to configure L2VPN quality of service (QoS) in port mode.

Configuring L2VPN Quality of Service Policy in Port Mode

This section describes how to configure L2VPN quality of service (QoS) in port mode.

Note In port mode, the interface name format does not include a subinterface number; for example, TenGigE0/3/0/5.20.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **interface** *type interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE0/3/0/5.20
```

Specifies the interface attachment circuit.

Step 3 **l2transport**

Example:

```
RP/0/RP0:hostname(config-if)# l2transport
```

Configures an interface or connection for L2 switching.

Step 4 **service-policy** [**input** | **output**] [policy-map-name]

Example:

```
RP/0/RP0:hostname(config-if)# service-policy input servpol1
```

Attaches a QoS policy to an input or output interface to be used as the service policy for that interface.

Step 5 **end or commit**

Example:

```
RP/0/RP0:hostname(config-if)# end
or
RP/0/RP0:hostname(config-if)# commit
```

- When you issue the end command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Preferred Tunnel Path

This procedure describes how to configure a preferred tunnel path.

Note The tunnel used for the preferred path configuration is an MPLS Traffic Engineering (MPLS-TE) tunnel.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters global configuration mode.

Step 2 **l2vpn**

Example:

```
RP/0/RP0:hostname(config)# l2vpn
```

Enters L2VPN configuration mode.

Step 3 **pw-class** *name*

Example:

```
RP/0/RP0:hostname(config-l2vpn)# pw-class path1
```

Configures the pseudowire class name.

Step 4 **encapsulation mpls**

Example:

```
RP/0/RP0:hostname(config-l2vpn-pwc)# encapsulation mpls
```

Configures the pseudowire encapsulation to MPLS.

Step 5 **preferred-path interface** [**tunnel-ip** *value* | **tunnel-te** *value* | **tunnel-tp** *value*] **fallback disable**

Example:

```
RP/0/RP0:hostname(config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te 11
fallback disable
```

Configures preferred path tunnel settings. If the fallback disable configuration is used and once the TE/TP tunnel is configured as the preferred path goes down, the corresponding pseudowire can also go down.

Note Ensure that fallback is supported.

Step 6 **end or commit**

Example:

```
RP/0/RP0:hostname(config-if)# end
or
RP/0/RP0:hostname(config-if)# commit
```

- When you issue the end command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

CHAPTER 45

VLAN over ODU

This chapter provides conceptual and configuration information to enable VLAN over ODU on Cisco NCS 4000 Series routers.

Understand VLAN over ODU

This feature enables the user to carry the VLAN traffic over the ODU channel. The ODU channel is created as part of the GMPLS tunnel using local termination method.

Local termination method enables the user to create multiple GMPLS tunnels from the head-end only instead of manually configuring tunnels across multiple nodes of the topology.

Local termination method is supported for following channelized interfaces:

- ODU4 terminating to 100GE interface.
- ODU2, ODU2e, ODU1e terminating to 10GE interface.
- ODU3 terminating to 40GE interface.

Enable VLAN over ODU : Configuring Head End Node

Following procedure enables to carry the VLAN traffic over an ODU channel. The ODU channel is created as part of the GMPLS tunnel using local termination method.

Procedure

Step 1 To configure an OTN controller,

Step 2 Configure GCC.

Step 3 Configure OSPF on the OTN controller, complete

Step 4 To configure packet controller :

Step 5 Perform manipulation of VLAN tags using rewrite command.

Step 6 To configure the MPLS-TE on packet controller, complete

Step 7 To configure local switching , complete Configuring Local Switching, on page 645.

SRLG Announce on Ethernet Terminated ODU

To provide better protection at L2 layer, the SRLG configured on OTN layer needs to be propagated to the Ethernet Terminated Interface. SRLG Announce feature enables to fetch SRLG values from all traversed TE-Links, summarize and announce them to the ethernet terminated interface at head and tail nodes.

Enabling SRLG Announce on Ethernet Terminated ODU

To provide better protection at L2 layer, the SRLG configured on OTN layer needs to be propagated to the Ethernet Terminated Interface. SRLG Announce feature enables to fetch SRLG values from all traversed TE-Links, summarize and announce them to the ethernet terminated interface at head and tail nodes.

Perform following procedure to enable SRLG announce on Ethernet Terminated ODU on headend node. SRLG announce can be enabled on both headend and tailend.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters Global Configuration mode.

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RP0:hostname(config)# mpls traffic-eng
```

Enters MPLS-TE configuration mode.

Step 3 **gmpls optical-nni**

Example:

```
RP/0/RP0:hostname(config-mpls-te)# gmpls optical-nni
```

Enters the GMPLS NNI configuration mode.

Step 4 **controller odu-group-te** *tunnel-id*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-nni)# controller odu-group-te 10
```

Enters the Odu-Group-Te configuration mode. The tunnel ID value ranges from 0 to 64535.

Step 5 **signalled-bandwidth** *oduk*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# signalled-bandwidth ODU2
```

Configures the bandwidth required for a GMPLS OTN tunnel.

Step 6 **static-uni local-termination interface-name** *interface-path-id* **remote-termination unnumbered** *tail-end-if-index*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# static-uni local-termination interface-name
TenGigE0/1/0/0/100 remote-termination unnumbered 32
```

Sets the static UNI endpoints of the NNI tunnel.

Step 7 **destination ipv4 unnumbered** *destination-router-id* **interface-ifindex** *destination-if-index*

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# destination ipv4 unnumbered 10.77.132.185
interface-if index 19
```

Specifies the GMPLS-NNI tunnel destination.

Step 8 **announce-srlg**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# announce-srlg
```

Enable Announce of SRLGs.

Step 9 **path-option** *path-option* **dynamic protected-by** *path-preference-level* **lockdown**

Example:

```
RP/0/RP0:hostname(config-te-gmpls-tun-0xa)# path-option 1 dynamic protected-by none lockdown
```

Sets path option for GMPLS NNI tunnel.

Enabling SRLG Announce on Ethernet Terminated ODU

The following example shows how to enable SRLG Announce on ethernet terminated ODU using Cisco IOS XR commands:

```
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
```

To verify the above configuration use the following show command:

```
 RP/0/RP0:hostname# show mpls tr 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
```

SRLG Inheritance of Packet Terminated Optical Controller

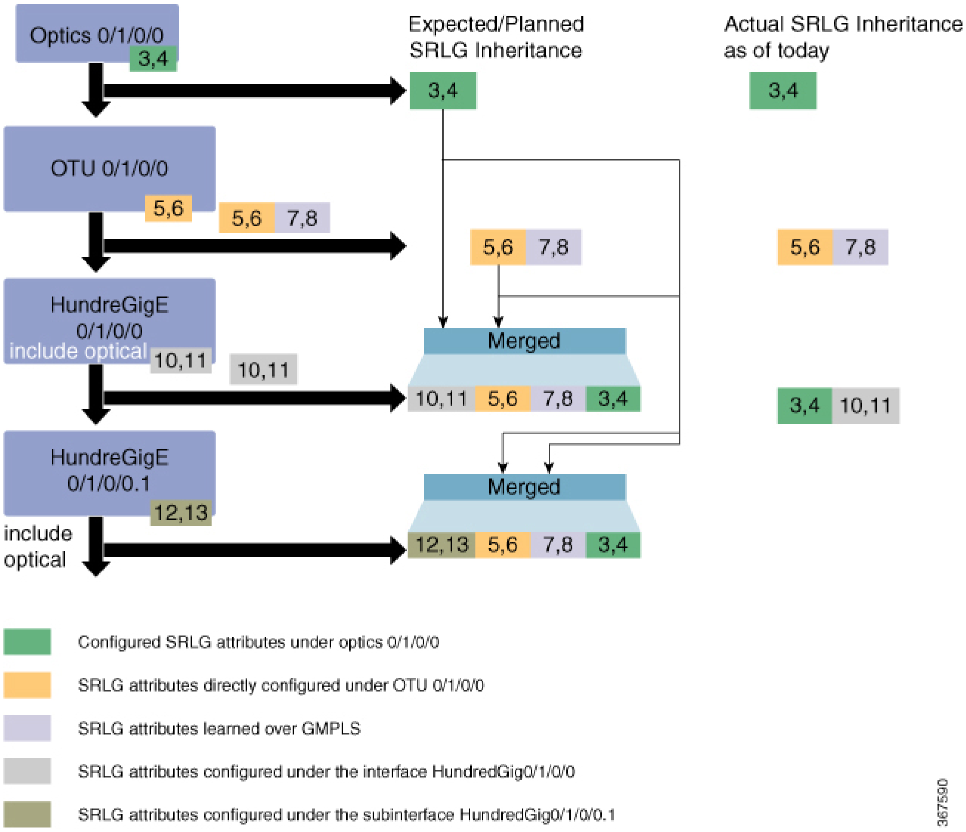
SRLG values configured under Controller Optics, Controller OTU and Controller ODU are inherited to its physical interfaces and subinterfaces.

RSI (RSI agent and RSI primary) maintain the optical database (DB) and the interface DB. The optical DB contains the SRLG values exported by producers while the interface DB contains the SRLG values configured by SRLG in itself. RSI primary acts as SRLG manager, which will handle SRLG values exported by existing as well as by new optical controllers and RSI agent uses these values to calculate the final set of SRLG values and send them to interested clients.

To inherit the SRLG values from controller OTU & ODU to the underlying physical interface, the SRLG values from Optical DB and Interface DB are merged. These values are merged by matching the R/S/I/P and giving SRLG values from immediate parent higher priority.

The following diagram summarizes the approach adopted to inherit the SRLG values:

Figure 35: Inheritance SRLG


Optics 0/1/0/0
3,4
Expected/Planned SRLG Inheritance
Actual SRLG Inheritance as of today
3,4
3,4
OTU 0/1/0/0
5,6
5,6
7,8
5,6
7,8
5,6
7,8
HundreGigE 0/1/0/0
include optical
10,11
10,11
Merged
10,11
5,6
7,8
3,4
3,4
10,11
HundreGigE 0/1/0/0.1
12,13
include optical
Merged
12,13
5,6
7,8
3,4
🟩 Configured SRLG attributes under optics 0/1/0/0
🟧 SRLG attributes directly configured under OTU 0/1/0/0
🟪 SRLG attributes learned over GMPLS
⬜ SRLG attributes configured under the interface HundredGig0/1/0/0
🟫 SRLG attributes configured under the subinterface HundredGig0/1/0/0.1
367590

CHAPTER 46

BGP Route Reflect

This chapter provides conceptual and configuration information to enable Border Gateway Protocol Route Reflect (BGP RR) on Cisco NCS 4000 Series routers.

Table 50: Feature History

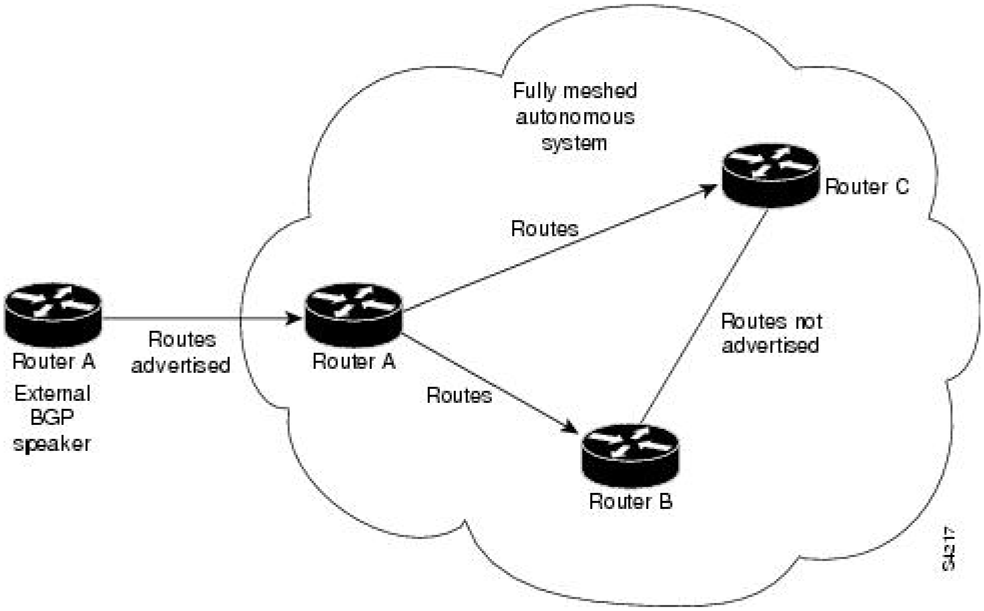
Feature Name	Release Information	Feature Description
BGP scale	Cisco IOS XR Release 6.5.31	BGP labeled unicast (BGP LU) supports 500 scale sessions with 8000 prefixes.

BGP Route Reflectors

BGP requires that all iBGP speakers be fully meshed. However, this requirement does not scale well when there are many iBGP speakers. Instead of configuring a confederation, you can reduce the iBGP mesh by using a route reflector configuration.

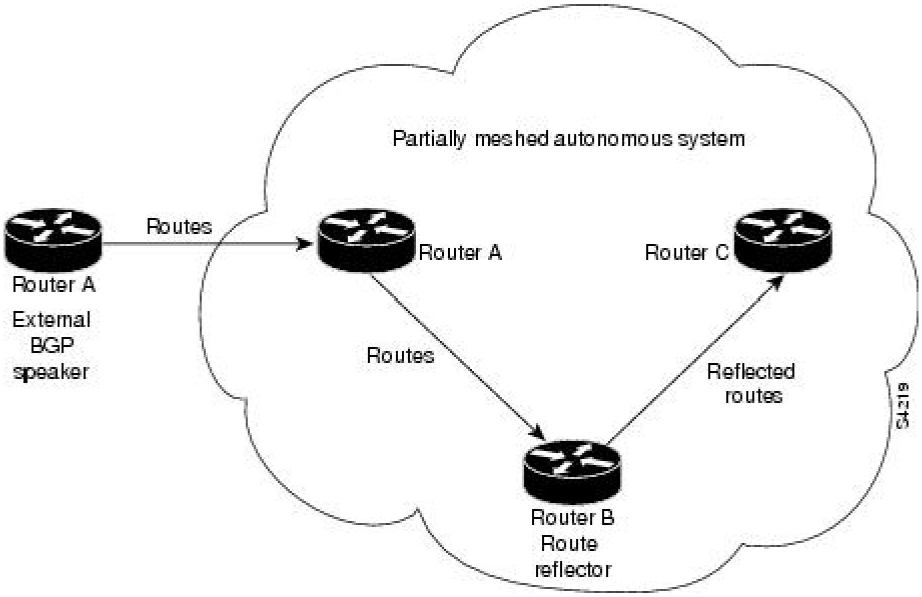
Figure below illustrates a simple iBGP configuration with three iBGP speakers (routers A, B, and C). Without route reflectors, when Router A receives a route from an external neighbor, it must advertise it to both routers B and C. Routers B and C do not readvertise the iBGP learned route to other iBGP speakers because the routers do not pass on routes learned from internal neighbors to other internal neighbors, thus preventing a routing information loop.

Figure 36: Three Fully Meshed iBGP Speakers



With route reflectors, all iBGP speakers need not be fully meshed because there is a method to pass learned routes to neighbors. In this model, an iBGP peer is configured to be a route reflector responsible for passing iBGP learned routes to a set of iBGP neighbors. In figure below, Router B is configured as a route reflector. When the route reflector receives routes advertised from Router A, it advertises them to Router C, and vice versa. This scheme eliminates the need for the iBGP session between routers A and C.

Figure 37: Simple BGP Model with a Route Reflector



The internal peers of the route reflector are divided into two groups: client peers and all other routers in the autonomous system (nonclient peers). A route reflector reflects routes between these two groups. The route reflector and its client peers form a *cluster*. The nonclient peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with iBGP speakers outside their cluster.

Figure 38: More Complex BGP Route Reflector Model

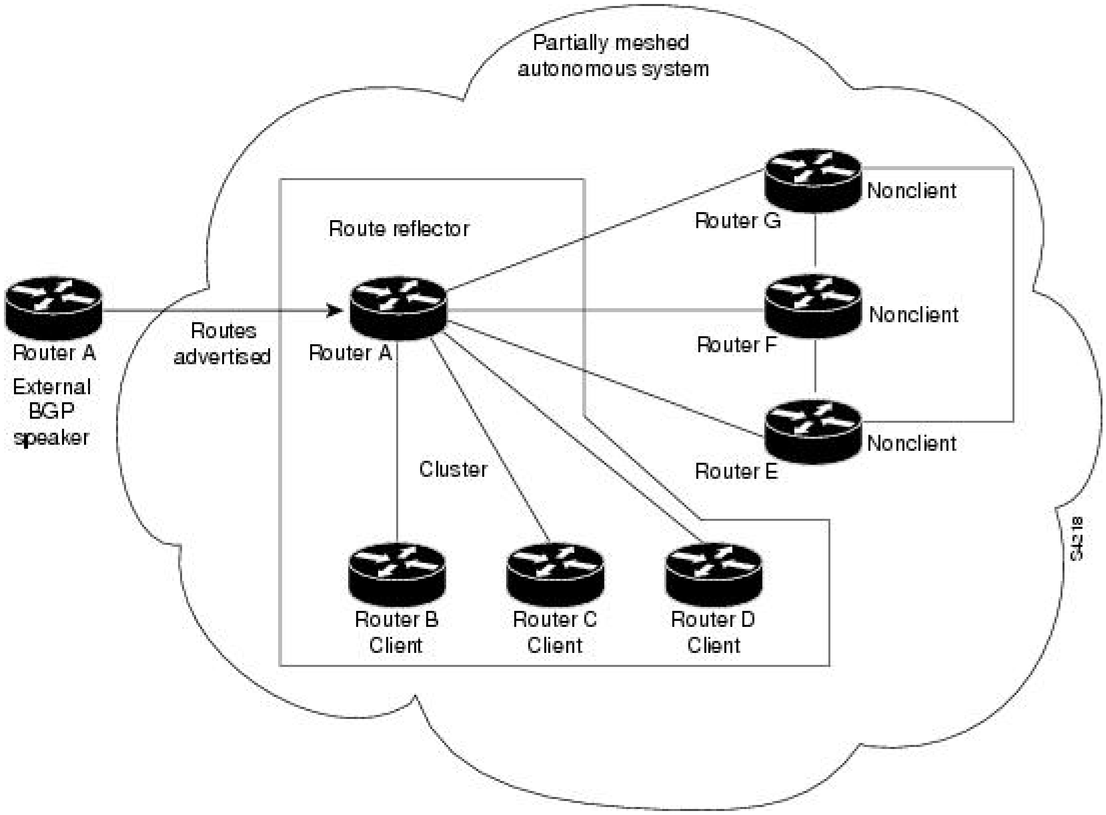


Figure above illustrates a more complex route reflector scheme. Router A is the route reflector in a cluster with routers B, C, and D. Routers E, F, and G are fully meshed, nonclient routers.

When the route reflector receives an advertised route, depending on the neighbor, it takes the following actions:

- A route from an external BGP speaker is advertised to all clients and nonclient peers.
- A route from a nonclient peer is advertised to all clients.
- A route from a client is advertised to all clients and nonclient peers. Hence, the clients need not be fully meshed.

Along with route reflector-aware BGP speakers, it is possible to have BGP speakers that do not understand the concept of route reflectors. They can be members of either client or nonclient groups, allowing an easy and gradual migration from the old BGP model to the route reflector model. Initially, you could create a single cluster with a route reflector and a few clients. All other iBGP speakers could be nonclient peers to the route reflector and then more clusters could be created gradually.

An autonomous system can have multiple route reflectors. A route reflector treats other route reflectors just like other iBGP speakers. A route reflector can be configured to have other route reflectors in a client group or nonclient group. In a simple configuration, the backbone could be divided into many clusters. Each route reflector would be configured with other route reflectors as nonclient peers (thus, all route reflectors are fully meshed). The clients are configured to maintain iBGP sessions with only the route reflector in their cluster.

Usually, a cluster of clients has a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. To increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. All route reflectors serving a cluster should be fully meshed and all of them should have identical sets of client and nonclient peers.

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, the route reflector need not reflect routes to clients.

As the iBGP learned routes are reflected, routing information may loop. The route reflector model has the following mechanisms to avoid routing loops:

- Originator ID is an optional, nontransitive BGP attribute. It is a 4-byte attributed created by a route reflector. The attribute carries the router ID of the originator of the route in the local autonomous system. Therefore, if a misconfiguration causes routing information to come back to the originator, the information is ignored.
- Cluster-list is an optional, nontransitive BGP attribute. It is a sequence of cluster IDs that the route has passed. When a route reflector reflects a route from its clients to nonclient peers, and vice versa, it appends the local cluster ID to the cluster-list. If the cluster-list is empty, a new cluster-list is created. Using this attribute, a route reflector can identify if routing information is looped back to the same cluster due to misconfiguration. If the local cluster ID is found in the cluster-list, the advertisement is ignored.

Table Policy

The table policy feature in BGP allows you to configure traffic index values on routes as they are installed in the global routing table. This feature is enabled using the **table-policy** command and supports the BGP policy accounting feature.

BGP policy accounting uses traffic indices that are set on BGP routes to track various counters.

Table policy also provides 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 result in an unwanted traffic drop where BGP advertises routes to neighbors that BGP does not install in its global routing table and forwarding table.

BGP Keychains

BGP keychains enable keychain authentication between two BGP peers. The BGP endpoints must both comply with draft-bonica-tcp-auth-05.txt and a keychain on one endpoint and a password on the other endpoint does not work.

BGP is able to use the keychain to implement hitless key rollover for authentication. Key rollover specification is time based, and in the event of clock skew between the peers, the rollover process is impacted. The configurable tolerance specification allows for the accept window to be extended (before and after) by that margin. This accept window facilitates a hitless key rollover for applications (for example, routing and management protocols).

The key rollover does not impact the BGP session, unless there is a keychain configuration mismatch at the endpoints resulting in no common keys for the session traffic (send or accept).

Configuring a Route Reflector for BGP

Perform this task to configure a route reflector for BGP.

All the neighbors configured with the **route-reflector-client** command are members of the client group, and the remaining iBGP peers are members of the nonclient group for the local route reflector.

Procedure

Step 1 **configure**

Step 2 **router bgp** *as-number*

Example:

```
RP/0/RP0:hostname(config)# router bgp 100
```

Specifies the autonomous system number and enters the BGP configuration mode, allowing you to configure the BGP routing process.

Step 3 **neighbor** *ip-address*

Example:

```
  RP/0/RP0:hostname(config-bgp)# neighbor 172.168.40.24
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.

Step 4 **remote-as** *as-number*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 2003
```

Creates a neighbor and assigns a remote autonomous system number to it.

Step 5 **keychain** *name*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)# keychain kych_a
```

Configures keychain-based authentication. Keychains provide secure authentication by supporting different MAC authentication algorithms and provide graceful key rollover.

Step 6 **update-source** *interface-type interface-id*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)# update-source Loopback 1
```

Allows sessions to use the primary IP address from a specific interface as the local address when forming a session with a neighbor. The interface-type interface-id arguments specify the type and ID number of the interface, such as TenGigEthernet or Loopback.

Step 7 **address-family { ipv4 | vpnv4 } labeled-unicast**

Example:

```
RP/0/RP0:hostname(config-nbr)# address-family ipv4 labeled-unicast
```

Specifies IPv4 or vpnv4 address family unicast and enters address family configuration submode.

Step 8 **route-reflector-client**

Example:

```
RP/0/RP0:hostname(config-bgp-nbr-af)# route-reflector-client
```

Configures the router as a BGP route reflector and configures the neighbor as its client.

Step 9 **commit**

Example:

The following example shows how to use an address family to configure internal BGP peer 6.6.6.6 as a route reflector client :

```
  RP/0/RP0:hostname# configure
  RP/0/RP0:hostname(config)# router bgp 100
  RP/0/RP0:hostname(config-bgp)# neighbor 6.6.6.6
  RP/0/RP0:hostname(config-bgp-nbr)# remote-as 100
  RP/0/RP0:hostname(config-bgp-nbr)# keychain kych_a
  RP/0/RP0:hostname(config-bgp-nbr)# update-source Loopback 1
  RP/0/RP0:hostname(config-bgp-nbr)# address-family ipv4 labeled-unicast
  RP/0/RP0:hostname(config-bgp-nbr-af)# route-reflector-client
```

Applying Table Policy

Perform this task to apply a routing policy to routes being installed into the routing table.

Procedure

Step 1 **configure**

Step 2 **router bgp** *as-number*

Example:

```
RP/0/RP0:hostname(config)# router bgp 100
```

Specifies the autonomous system number and enters the BGP configuration mode, allowing you to configure the BGP routing process.

Step 3 **address-family { ipv4 | vpnv4 } unicast**

Example:

```
RP/0/RP0:hostname(config-bgp)# address-family ipv4 unicast
```

Specifies the IPv4 or vpnv4 address family and enters address family configuration submode.

Step 4 **table-policy** *policy-name*

Example:

```
RP/0/RP0:hostname(config-bgp-af)# table-policy drop-all
```

Applies the specified policy to routes being installed into the routing table.

Step 5 **commit**

Example:

The following example shows how to apply the drop-all policy to IPv4 unicast routes being installed in the routing table :

```
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)# table-policy drop-all
```

Configuring BGP Route Reflect Filtering by Table Policy

Perform this task to configure BGP route reflect filtering by table policy.

Procedure

Step 1 **configure**

Step 2 **router bgp** *as-number*

Example:

```
RP/0/RP0:hostname(config)# router bgp 100
```

Specifies the autonomous system number and enters the BGP configuration mode, allowing you to configure the BGP routing process.

Step 3 **address-family { ipv4 | vpnv4 } unicast**

Example:

```
RP/0/RP0:hostname(config-bgp)# address-family ipv4 unicast
```

Specifies the IPv4 or vpnv4 address family and enters address family configuration submode.

Step 4 **table-policy** *policy-name*

Example:

```
RP/0/RP0:hostname(config-bgp-af)# table-policy drop-all
```

Applies the specified policy to routes being installed into the routing table.

Step 5 **exit**

Example:

```
RP/0/RP0:hostname(config-bgp-af)# exit
```

Exits the current configuration mode.

Step 6 **neighbor** *ip-address*

Example:

```
  RP/0/RP0:hostname(config-bgp)# neighbor 172.168.40.24
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.

Step 7 **remote-as** *as-number*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 2003
```

Creates a neighbor and assigns a remote autonomous system number to it.

Step 8 **keychain** *name*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)# keychain kych_a
```

Configures keychain-based authentication. Keychains provide secure authentication by supporting different MAC authentication algorithms and provide graceful key rollover.

Step 9 **update-source** *interface-type interface-id*

Example:

```
RP/0/RP0:hostname(config-bgp-nbr)# update-source Loopback 1
```

Allows sessions to use the primary IP address from a specific interface as the local address when forming a session with a neighbor. The interface-type interface-id arguments specify the type and ID number of the interface, such as TenGigEthernet or Loopback.

Step 10 **address-family { ipv4 | vpnv4 } labeled-unicast**

Example:

```
RP/0/RP0:hostname(config-nbr)# address-family ipv4 labeled-unicast
```

Specifies IPv4 or vpnv4 address family unicast and enters address family configuration submode.

Step 11 **route-reflector-client**

Example:

```
RP/0/RP0:hostname(config-bgp-nbr-af)# route-reflector-client
```

Configures the router as a BGP route reflector and configures the neighbor as its client.

Step 12 **commit**

Example:

The following example shows how to use an address family to configure internal BGP peer 100.4.1.1 as a route reflect filter by table policy client:

```
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)# table-policy drop-all
RP/0/RP0:hostname(config-bgp-af)# exit
RP/0/RP0:hostname(config-bgp)# neighbor 100.4.1.1
RP/0/RP0:hostname(config-bgp-nbr)# remote-as 100
RP/0/RP0:hostname(config-bgp-nbr)# keychain kych_b
RP/0/RP0:hostname(config-bgp-nbr)# update-source Loopback 1
RP/0/RP0:hostname(config-bgp-nbr)# address-family ipv4 labeled-unicast
RP/0/RP0:hostname(config-bgp-nbr-af)# route-reflector-client
```

Verifying BGP

Perform this task to verify BGP configuration.

Procedure

Step 1 **show bgp summary**

Example:

```
RP/0/RP0:hostname# show bgp summary
```

Displays the status of all BGP connections.

Step 2 **show bgp ipv4 labeled-unicast summary**

Example:

```
RP/0/RP0:hostname# show bgp ipv4 labeled-unicast summary
```

Step 3 **show bgp neighbors**

Example:

```
RP/0/RP0:hostname# show bgp neighbors
```

Displays the information about BGP connections to neighbors.

Step 4 **show bgp paths detail**

Example:

```
RP/0/RP0:hostname# show bgp paths detail
```

Displays all the BGP paths in the database.

Step 5 **show bgp route-policy** *route-policy-name*

Example:

```
RP/0/RP0:hostname# show bgp route-policy p1
```

Displays the BGP information about networks that match an outbound route policy.

Step 6 **show bgp policy**

Example:

```
RP/0/RP0:hostname# show bgp policy
```

Displays the information about BGP advertisements under a proposed policy.

Step 7 **show bgp advertised neighbor** *ip-address* **summary**

Example:

```
RP/0/RP0:hostname# show bgp advertised neighbor 10.0.101.4 summary
```

Displays the advertisements for neighbors or a single neighbor.

BGP Labeled Unicast

BGP labeled unicast (LU) enables MPLS transport across IGP boundaries. By advertising loopbacks and label bindings across IGP boundaries, we can communicate to other routers in remote areas that are not part of our local IGP. BGP LU advertisements only impact edge routers and border routers.

Let us consider a network with three different areas: one core and two aggregation areas on the side. Each area runs its own IGP, with no redistribution between them on the Area Border Router (ABR). Use of BGP is needed in order to provide an end-to-end MPLS LSP. BGP advertises the loopbacks of the PE routers with a label across the whole domain, and provides an end-to-end LSP. BGP is deployed between the PEs and ABRs with BGP Labeled Unicast.

The NCS4K-4H-OPW-QC2 line card supports BGP LU.

Advantages of BGP LU

Following are the advantages of BGP LU:

- With BGP LU, routes and labels are carried together and this increases the scalability.
- Enables filtering of next-hop loops, thereby reducing the labels advertised by LDP/ RSVP.
- Reduction of OSPF/ ISIS and LDP/RSVp databases.
- Enables establishing an end-to-end label path across domains.

Limitations of BGP LU

Following are the limitations of BGP LU:

- When PW uses BGP LU for signaling, preferred path is not supported.
- BGP LU is supported on the NCS4K-2H10T-OP-KS line card only in the OTN mode. Use the **hw-module profile otn 200g-slot-otn-only** command to enable BGP LU and this command places the line card in the OTN mode.
- When MPLS activate is configured between two directly connected BGP LU nodes, then a static route must be used to create end to end PW.

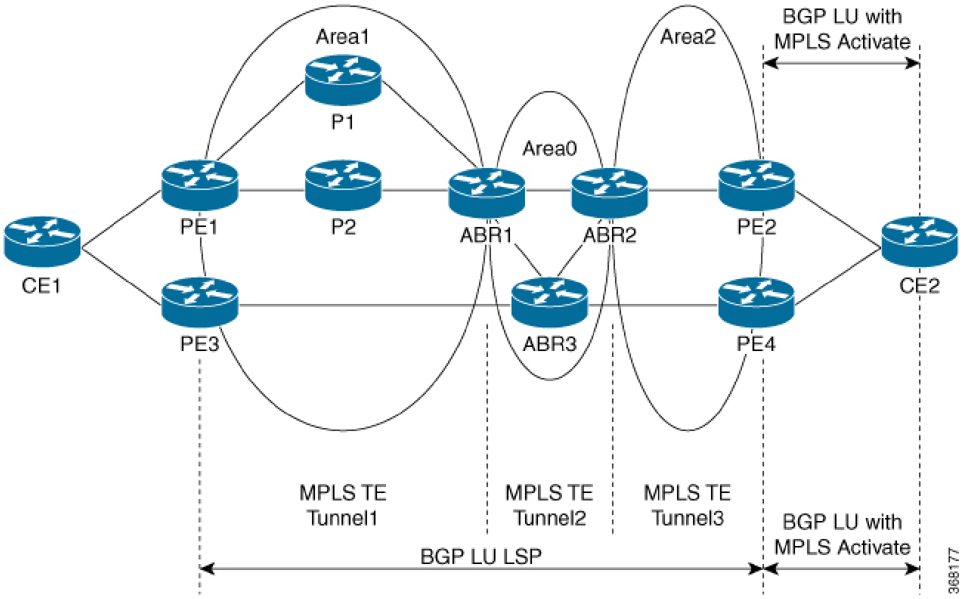
BGP LU Scale Details

In Release 6.5.31, BGP LU supports 500 scale sessions with 8000 prefixes.

Implementing BGP LU

Some of the use cases for BGL LU are discussed here. With reference to the below figure, consider BGP LU runs on the PE and the ABR routers (and not on the P routers). The IGP protocol used can be OSPF or ISIS.

Figure 39: Implementing BGP LU



- IP over BGP LU LSP over LDP - the IP packets are encapsulated with two labels (BGP label and the LDP label) from PE1 and sent to P2. The packet reaches with BGP label in ABR1. In ABR1, the BGP label is swapped and the packet reaches ABR2, only with the swapped BGP label. In ABR2, BGP label again gets swapped to reach PE2. PE2 acts like a PHP where the BGP label is popped before sending the packet to CE2.
- IP over BGP LU LSP over MPLS TE - the packet path is the same as discussed above. Here the IGP area has MPLS TE tunnels as transport.
- IP over BGP LU with TE tunnels with link/node protection FRR path - the packet path is the same , but in case of link failure (PE1 to P) or node failure (P), TE FRR on the PE1 takes the back up path (which

is, PE2-P1-ABR1). In this case, the packet has three labels (BG label, TE label, Mergepoint label) to reach ABR1.

- VPWS ober BGP LU with TE tunnels - here, the VPWS service uses the BGP LU labelled path as transport to carry the pseudowires. The VC label is also added to the label stack. The back-up path includes four labels (VC-label, BGP label, TE label, MP label).

BGP Prefix Independent Convergence

The Border Gateway Protocol Prefix Independent Convergence Unipath (BGP PIC Unipath) primary/backup feature provides the capability to install a backup path into the forwarding table. Installing the backup path provides prefix independent convergence in the event of a primary PE–CE link failure.

The primary/backup path provides a mechanism for BGP to determine a backup best path. The backup best path acts as a backup to the overall best path, which is the primary best path. BGP installs the primary path and the backup path in the RIB, and the FIB programs the primary backup path in the hardware. FIB is responsible for triggering prefix independent convergence based on the IGP update in the RIB.

The procedure to determine the backup best path is as follows:

- Determine the best path from the entire set of paths available for a prefix.
- Eliminate the current best path.
- Eliminate all the paths that have the same next hop as that of the current best path.

The PE-CE local convergence is in the order of four to five seconds for 10000 prefixes. Installing a backup path on the linecards, so that the Forwarding Information Base (FIB) can immediately switch to an alternate path, in the event of a primary PE-CE link failure reduces the convergence time. There are two types of BGP PICs:

- BGP PIC Core: ensures BGP traffic converges quickly when there is a change in the IGP path to the BGP next hop. It addresses failures in the core where the recursive BGP path stays intact and when BGP LU neighbors are unaffected. Failures covered are P-PE link or P node failures that trigger a change of the IGP path to the BGP next-hop.
- BGP PIC Edge: here, BGP pre-computes both primary and backup paths for a prefix and installs them into the RIB/FIB. The fast convergence is invoked when the route to the primary next hop goes down. CEF/FIB modifies a shared object to indicate that the repair path must be used instead of the primary, thus preventing the need to update many BGP prefixes.

BGP LU and PIC Configuration

Perform this task to install a backup path into the forwarding table and provide prefix independent convergence (PIC) in case of a PE-CE link failure.

Procedure

Step 1 **configure**

Enters global configuration mode.

Step 2 **router bgp** *as-number*

Example:

```
RP/0/CPU0:router(config)# router bgp 100
```

Specifies the autonomous number and enters the BGP configuration mode.

Step 3 **address-family ipv4**

Example:

```
RP/0/CPU0:router(config-bgp)# address-family ipv4
```

Enters the address-family configuration mode.

Step 4 **neighbor** *ip address* **remote-as** *as_number* **address-family ipv4 label-unicast**

Example:

```
RP/0/CPU0:router(config-bgp-af)# neighbor 20.20.20.20
  remote-as 1
  update-source Loopback1
  address-family ipv4 label-unicast
   route-policy pass-all in
   route-policy pass-all out
```

Enables connecting to BGP LU neighbors.

Step 5 **additional-paths selection route-policy** *policy-name*

Example:

```
RP/0/CPU0:router(config-bgp-af)# additional-paths selection route-policy p1
```

Configures additional paths selection mode for a prefix. This calculates the backup paths and enables PIC.

Step 6 **commit**

Saves the configuration changes made.

CHAPTER 47

Configure Smart Licensing

This chapter describes the procedures to configure smart licensing.

For more information about smart licensing, see Smart Licensing Overview, on page 131.

For more information about the consumption model, see Consumption Model, on page 134.

Configure Smart Software Licensing Using CLI

Perform these steps to register or deregister the device. You can also manually renew the ID certificate and authorization.

Before you begin

You must have purchased the product for which you are adding the license. When you purchase the product, you are provided with a user name and password to the Cisco Smart Software Manager portal, from where you can generate the product instance registration tokens.

Procedure

Step 1 To register the device, perform Steps 5 through 8.

Step 2 To deregister the device, perform Step 9.

Step 3 To renew ID certificate, perform Step 10.

Step 4 To renew authorization, perform Steps 11.

Step 5 Login to your smart account in Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory) or smart software manager satellite using the Cisco provided username and password.

Step 6 Generate a product instance registration token. Copy or download the token to a text file.

The token is used to register and activate a device, and assign the device to a virtual account.

Step 7 **license smart register idtoken** *token_ID*

Example:

```
RP/0/RP0:hostname# license smart register idtoken YTk3NmVlYTAtODNlMy00NGZjLTgxN$
License command "license smart register idtoken " completed successfully.
Registration process is in progress. Use the 'show license status' command to check the
progress and result
```

In case the token is invalid, the initial registration fails.

```
RP/0/RP0:hostname#%SMART_LIC-3-AGENT_REG_FAILED:Smart Agent for Licensing Registration with
 Cisco licensing cloud failed: Response error: {"token":["The token
'YTk3NmVlYTAtODNlMy00NGZjLTgxNTQtMjNkOGFjZjJiZjAxLTE1MDAxMDQx%0AMTE0MDF8bFRvVmRFYjhPaFdKSmVmT3ZiSEVxbVJxUkRTRW91ellMZHhONGMr%0ATEMvOD0%3'
 is not valid."]}
```

In case there is a communication failure between the device and the portal or satellite, the registration fails as seen in the example below. CTC waits for 24 hours before attempting to register the device again. To force the registration, perform Step 8.

```
RP/0/RP0:hostname # show license status
Wed Jun  7 02:20:49.377 UTC
Smart Licensing is ENABLED
  Initial Registration: FAILED on Tue Jun 06 2017 23:50:17 UTC
    Failure reason: Fail to send out Call Home HTTP message

License Authorization:
  Status: No Licenses in Use
```

Step 8 **license smart register idtoken** *token_ID* force

Example:

```
RP/0/RP0:hostname# license smart register idtoken YTk3NmVlYTAtODNlMy00NGZjLTgxN$ force
License command "license smart register idtoken " completed successfully.
Registration process is in progress. Use the 'show license status' command to check the
progress and result
```

Step 9 **license smart deregister**

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 the **license smart deregister** command to cancel the registration on your device. All smart licensing entitlements and certificates on the platform are removed.

Note Though the product instance has been de-registered from the Cisco license cloud service, smart licensing is still enabled.

Example:

```
RP/0/RP0:hostname#license smart deregister
Wed Jun  7 14:56:04.312 UTC

License command "license smart deregister " completed successfully.
```

Step 10 **license smart renew 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.

Example:

```
RP/0/RP0:hostname#license smart renew id
Fri Jun  9 05:11:18.982 UTC
```

```
Id certificate renew process is in progress. Use the 'show license status' command to check
 the progress and result
```

Step 11 **license smart renew 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 the **license smart renew auth** 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 issue this command 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 the **license smart renew auth** command to retry the authorization period renewal. If the retry is successful, a new authorization period begins.

Example:

```
RP/0/RP0:hostname#show license all
Mon Jun 12 15:17:19.805 UTC

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: NCS4K
  Virtual Account: NCS4K-VIRTUAL-AC
  Initial Registration: SUCCEEDED on Mon Jun 12 2017 15:12:35 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sat Dec 09 2017 15:14:50 UTC
  Registration Expires: Tue Jun 12 2018 09:45:25 UTC

License Authorization:
  Status: AUTH EXPIRED on Mon Jun 12 2017 15:15:27 UTC
  Last Communication Attempt: SUCCEEDED on Mon Jun 12 2017 15:15:27 UTC
  Next Communication Attempt: Mon Jun 12 2017 16:16:49 UTC
  Communication Deadline: DEADLINE EXCEEDED

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: AUTH EXPIRED

NCS4K 100G Bandwidth Licenses (S-NCS4K-100G-LIC):
  Description: NCS4K 100G Bandwidth Licenses
  Count: 2
  Version: 1.0
  Status: AUTH EXPIRED

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: AUTH EXPIRED

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
```

To manually renew the authorization, use the **license smart renew auth** command.

Example:

```
RP/0/RP0:hostname#license smart renew auth
Fri Jun  9 10:55:43.262 UTC
Authorization process is in progress. Use the 'show license status' command to check the
progress and result
```

What to do next

You can use the show commands to verify the default Smart Licensing configuration. If any issue is detected, take corrective action before making further configurations.

Verify Smart Licensing Configuration Using CLI

Use the show commands to verify the default smart licensing configuration.

Procedure

Step 1 **show license status**

Displays the compliance status of Smart Licensing. The following status are reported:

- **Authorized:** Indicates that your device is able to communicate with the Cisco license manager, and is authorised to initiate requests for license entitlements.
- **Out-Of-Compliance:** Indicates that one or more of your licenses are out-of-compliance. You must buy additional licenses.

Example:

Output 1

```
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 05:40:12 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mon Dec 04 2017 05:40:11 UTC
  Registration Expires: Thu Jun 07 2018 05:37:25 UTC

License Authorization:
  Status: OUT OF COMPLIANCE on Wed Jun 07 2017 05:40:28 UTC
  Last Communication Attempt: SUCCEEDED on Wed Jun 07 2017 05:40:28 UTC
  Next Communication Attempt: Wed Jun 07 2017 17:40:27 UTC
  Communication Deadline: Tue Sep 05 2017 05:37:42 UTC
```

Example:

Output 2:

```
RP/0/RP0:hostname# show license status
Wed Jun  7 12:08:09.919 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
```

Step 2 **show license summary**

Example:

```
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
```

Step 3 **show license all**

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.

Example:

```
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
```

Step 4 **show alarms brief system active**

The following conditions are reported if:

- One or more entitlements are out of compliance (LICENSE-OUT-OF-COMPLIANCE): This alarm is raised when the license consumption is more than the licenses that have been allocated in the Cisco Smart Software Manager (CSSM) license cloud server. The alarm is cleared when more licenses are purchased and updated in the CSSM license cloud server.

- Communication to the cloud server failure (LICENSE-COMM-FAIL): This alarm is raised when the router is not able to communicate with the CSSM license cloud server. The alarm is cleared. when the communication is restored.

Example:

```
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
```

Configuring Call Home HTTP Proxy Server Using CLI

Perform these steps to configure the HTTP proxy server.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Step 2 **call-home**

Enters the call home configuration mode.

Example:

```
RP/0/RP0:hostname(config)# call-home
RP/0/RP0:hostname(config-call-home)#
```

Step 3 **http-proxy** *proxy-server-name* **port** *port-number*

Configures the port for the specified HTTP proxy server. Range is 1 to 65535.

Example:

```
RP/0/RP0:hostname(config)# call-home
RP/0/RP0:hostname(config-call-home)#http-proxy aa.bbb.cc.dd port 100
```

Step 4 **commit**

Configuring and Activating Call Home Destination Profiles Using CLI

Perform these steps to configure and activate a destination profile.

Before you begin

You must have at least one activated destination profile for Call Home messages to be sent. The CiscoTAC-1 profile exists by default and is active. To create and activate a different profile, perform the following steps.

Note Before you activate the new profile, you need to deactivate the CiscoTAC-1 profile using the **no active** command.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Step 2 **call-home**

Enters the call home configuration mode.

Example:

```
RP/0/RP0:hostname(configure)# call-home
RP/0/RP0:hostname(configure-call-home)#
```

Step 3 **profile** *profile-name*

Enters call home profile configuration mode to configure a new or existing profile.

Example:

```
RP/0/RP0:hostname(configure-call-home)# profile my-profile
RP/0/RP0:hostname(configure-call-home-profile)#
```

Step 4 **destination address http** *http-address-url*

Configures a destination URL to which Call Home and Smart Licensing messages are sent for this profile.

Example:

```
RP/0/RP0:hostname(configure-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Step 5 **reporting** {**all | smart-call-home-data | smart-licensing-data** }

The smart call home data, smart licensing data, or both are reported to the CSSM.

Example:

```
RP/0/RP0:hostname(configure-call-home-profile)# reporting smart-call-home-data
RP/0/RP0:hostname(configure-call-home-profile)# reporting smart-licensing-data
```

Step 6 **destination transport-method [email | http]**

Configures the transport method for this profile. Use http if the profile is used for sending Smart Licensing messages.

Example:

```
RP/0/RP0:hostname(configure-call-home-profile)# destination
transport-method http
```

Step 7 **active**

Activates the destination profile.

Note At least one destination profile must be active for Call Home messages to be sent.

Step 8 **commit**

Step 9 **show call-home profile** {**all** | *profile-name* }

Displays information about the destination profile.

Example:

```
RP/0/RP0:hostname# show call-home profile all
```

CHAPTER 48

Configure Link Aggregation

This chapter describes the procedures to configure Link Aggregation on Cisco NCS 4000 Series routers.

Link Aggregation Overview

Link Aggregation (LAG) is a mechanism used to aggregate physical interfaces or ports to create a logical entity called link bundle.

Traditionally LAG is a trunking technology that groups together multiple full-duplex IEEE 802.3 Ethernet interfaces to provide fault-tolerant high-speed links between switches, routers, and servers. LAG forms a single higher bandwidth routing or bridging endpoint and was designed primarily for host-to-switch connectivity. Following are the benefits:

- Logical aggregation of bandwidth
- Load balancing
- Fault tolerance

In NCS 4000 Series Routers, primary application of LAG is to provide connectivity to Access devices like NCS4200 Series and on the core side provide connectivity to Multi-service Edge (NCS 6000 Series) and Core Routers (like NCS 6000 Series).

Understanding Link Bundle

A link bundle is a group of one or more ports that are aggregated or bundled together and act as a single link. This single link can be treated as a main interface or as a VLAN subinterface.

The advantages of link bundles are these:

- Multiple links can span several line cards to form a single interface. Thus, the failure of a single link does not cause a loss of connectivity.
- Bundled interfaces increase bandwidth availability, because traffic is forwarded over all available members of the bundle. Therefore, traffic can flow on the available links if one of the links within a bundle fails. Bandwidth can be added without interrupting packet flow.

NCS 4000 Series XR software supports following methods of forming bundles of Ethernet interfaces:

- IEEE 802.3ad—Standard technology that employs a Link Aggregation Control Protocol (LACP) to ensure that all the member links in a bundle are compatible. Links that are incompatible or have failed are automatically removed from a bundle.
- Static-LAG—Cisco proprietary technology that allows the user to configure links to join a bundle, but has no mechanisms to check whether the links in a bundle are compatible.

Characteristics and Limitations of Link Bundles

This list describes the properties and limitations of link bundles:

- 10 Gigabit, 40 Gigabit, and 100 Gigabit Ethernet interfaces can be bundled, with or without the use of LACP (Link Aggregation Control Protocol).
- Bundle membership can span across several line cards that are installed in the same chassis for NCS4000.
- The Cisco NCS 4000 Series Router supports a maximum of 128 Ethernet link bundles, 1000 Ethernet link bundles sub-interfaces. Each link bundle can have a maximum of 16 physical links.
- All the members in a link bundle shall be of same speed.
- Physical layer and link layer configuration are performed on individual member at physical interface layer.
- Configuration of network layer protocols and higher layer applications is performed on the bundle itself.
- A bundle can be administratively enabled or disabled.
- Each individual link within a bundle can be administratively enabled or disabled.
- Bundle member links are not supported on OTN terminated interfaces.
- Load balancing (the distribution of data between member links) is done with source and destination mac address.

Note Load balancing is done based on each stream, so each interface in the bundle may not carry equal traffic.

- QoS is supported and can be applied on the bundle interface and sub interfaces.
- LAG CFM is supported and can be applied on the bundle interface and subinterfaces.
- LAG is only supported for both L2 and L3 interfaces.

- Link layer protocols, such as LLDP and Link OAM , work independently on each link within a bundle.
- Upper layer protocols, such as routing updates and hellos, are sent over any member link of an interface bundle.
- Bundled interfaces are point to point.
- All links within a single bundle must be configured either to run 802.3ad (LACP) or Static-LAG (non-LACP). Mixed links within a single bundle are not supported.
- Only default LACP timer (30sec) is supported.
- To provision EVPL service with Bundle AC, user has to provision the bundle main interface along with the L2 bundle sub-interfaces. QOS or any other feature over the bundle main interface needs to be configured once the EVPL service is provisioned.
- When link-OAM is configured on the bundle interface, its recommended to configure one of the following command options:
    - `RP/0/RP0:hostname(config)# ethernet oam profile <profile name> action wiring-conflict disable`
    - `RP/0/RP0:hostname(config)# ethernet oam profile <profile name> action wiring-conflict efd`
    - `RP/0/RP0:hostname(config)# ethernet oam profile <profile name> action wiring-conflict log`
- While performing RPVM Switch Over or RP OIR or ISSU, the packet transmission stops for a duration of 3 to 20 seconds and causes CFM sessions with CCM interval 1 second and 10 seconds to flap (session goes down and recovers back).

IEEE 802.3ad Standard

The IEEE 802.3ad standard typically defines a method of forming Ethernet link bundles.

For each link configured as bundle member, this information is exchanged between the systems that host each end of the link bundle:

- A globally unique local system identifier
- An identifier (operational key) for the bundle of which the link is a member
- An identifier (port ID) for the link
- The current aggregation status of the link

This information is used to form the link aggregation group identifier (LAG ID). Links that share a common LAG ID can be aggregated. Individual links have unique LAG IDs.

The system identifier distinguishes one router from another, and its uniqueness is guaranteed through the use of a MAC address from the system. The bundle and link identifiers have significance only to the router assigning them, which must guarantee that no two links have the same identifier, and that no two bundles have the same identifier.

The information from the peer system is combined with the information from the local system to determine the compatibility of the links configured to be members of a bundle.

Bundle MAC addresses in the routers come from a set of reserved MAC addresses in the backplane. This MAC address stays with the bundle as long as the bundle interface exists. The bundle uses this MAC address until the user configures a different MAC address. The bundle MAC address is used by all member links when passing bundle traffic. Any unicast or multicast addresses set on the bundle are also set on all the member links.

Note We recommend that you avoid modifying the MAC address, because changes in the MAC address can affect packet forwarding.

Prerequisites for Configuring LAG

Before configuring LAG, be sure that these tasks and conditions are met:

- 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.

- You know the interface IP address (Layer 3 only).

- You know which links should be included in the bundle you are configuring.

- If you are configuring an Ethernet link bundle, you should have NCS4K-4H-OPW-QC2 line card installed in the router.

VLAN Subinterfaces on an Ethernet Link Bundle

802.1Q VLAN subinterfaces can be configured on 802.3ad Ethernet link bundles. The maximum number of VLAN subinterfaces allowed per router is 1024 minus the number of main interface(s) configured. Example if one main bundle is configured then maximum 1023 VLAN subinterface bundles can be configured on the router.

Note The memory requirement for bundle VLANs is slightly higher than standard physical interfaces.

To create a VLAN subinterface on a bundle, include the VLAN subinterface instance with the **interface Bundle-Ether** command:

interface Bundle-Ether `instance.subinterface`

After you create a VLAN on an Ethernet link bundle, all physical VLAN subinterface configuration is supported on that link bundle.

Link Aggregation Through LACP

Aggregating interfaces on different line cards provides redundancy, allowing traffic to be quickly redirected to other member links when an interface or modular services card failure occurs.

The optional Link Aggregation Control Protocol (LACP) is defined in the IEEE 802 standard. LACP communicates between two directly connected systems (or peers) to verify the compatibility of bundle members. For the Cisco NCS 4000 Series Routers, the peer can be either another router or a switch. LACP monitors the operational state of link bundles to ensure these:

- All links terminate on the same two systems.
- Both systems consider the links to be part of the same bundle.
- All links have the appropriate settings on the peer.

LACP transmits frames containing the local port state and the local view of the partner system's state. These frames are analyzed to ensure both systems are in agreement.

How to Configure Link Bundling

Configuring Ethernet Link Bundles

This section describes how to configure a Ethernet link bundle.

Note MAC accounting is not supported on Ethernet link bundles.

Note In order for an Ethernet bundle to be active, you must perform the same configuration on both connection endpoints of the bundle.

The creation of an Ethernet link bundle involves creating a bundle and adding member interfaces to that bundle, as shown in the steps that follow.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the XR Config mode.

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 3
```

Creates and names a new Ethernet link bundle.

Step 3 **bundle minimum-active bandwidth** *kbps*

Example:

```
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 580000
```

(Optional) Sets the minimum amount of bandwidth required before a user can bring up a bundle.

Step 4 **bundle minimum-active links** *links*

Example:

```
RP/0/RP0:hostname(config-if)# bundle minimum-active links 2
```

(Optional) Sets the number of active links required before you can bring up a specific bundle.

Step 5 **bundle maximum-active links** *links*

Example:

```
RP/0/RP0:hostname(config-if)# bundle maximum-active links 1
```

(Optional) Designates one active link and one link in standby mode that can take over immediately for a bundle if the active link fails (1:1 protection).

The default number of active links in a single bundle is 8.

Note If the **bundle maximum-active** command is issued, then only the highest-priority link within the bundle is active. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, we recommend that you configure a higher priority on the link that you want to be the active link.

Step 6 **bundle maximum-active links** *links* **hot-standby**

Example:

```
RP/0/RP0:hostname(config-if)# bundle maximum-active links 1 hot-standby
```

The **hot-standby** keyword helps to avoid bundle flaps on a switchover or switchback event during which the bundle temporarily falls below the minimum links or bandwidth threshold.

It sets default values for the wait-while timer and suppress-flaps timer to achieve this.

Step 7 **l2transport**

Example:

```
RP/0/RP0:hostname(config-if)# l2transport
```

Note Bundled interfaces are supported only in L2transport mode.

Step 8 **lacp system priority** *value*

Example:

```
RP/0/RP0:hostname(config-if)# lacp system priority ?
<1-65535>  Bundle LACP system priority. Lower value is higher priority.
RP/0/RP0:hostname(config-if)#lacp system priority 1000
RP/0/RP0:hostname(config-if)#commit
RP/0/RP0:HEADRP/0/RP0:hostname(config-if)#end
RP/0/RP0:hostname#
```

Sets the system priority for Ethernet link bundle.

Step 9 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration submode for the Ethernet link bundle.

Step 10 **interface** { **TenGigE** | **HundredGigE** } *instance*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 1/0/0/0
```

Enters the interface configuration mode for the specified interface.

Mixed bandwidth bundle member configuration is only supported when 1:1 redundancy is configured.

Note Mixed link bundle mode is supported only when active-standby operation is configured (usually with the lower speed link in standby mode).

Step 11 **bundle id** *bundle-id* [**mode** { **active** | **on** | **passive**}]

Example:

```
RP/0/RP0:hostname(config-if)# bundle-id 3
```

Adds the link to the specified bundle.

To enable active or passive LACP on the bundle, include the optional **mode active** or **mode passive** keywords in the command string.

To add the link to the bundle without LACP support, include the optional **mode on** keywords with the command string.

Note If you do not specify the **mode** keyword, the default mode is **on** (LACP is not run over the port).

Step 12 **no shutdown**(optional)

Example:

```
RP/0/RP0:hostname(config-if)# no shutdown
```

If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up or down state depending on the configuration and state of the link.

Step 13 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration submode for the Ethernet link bundle.

Step 14 Repeat Step 8 through Step 11 to add more links to the bundle you created in Step 2.

Step 15 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Step 16 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration mode.

Step 17 **exit**

Example:

```
RP/0/RP0:hostname(config)# exit
```

Exits the XR Config mode.

Step 18 Perform Step 1 through Step 15 on the remote end of the connection.

Brings up the other end of the link bundle.

Step 19 **show bundle Bundle-Ether** *bundle-id* [**reasons**] (optional)

Example:

```
RP/0/RP0:hostname# show bundle Bundle-Ether 3 reasons
```

Shows information about the specified Ethernet link bundle

Step 20 **show lacp Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname # show lacp Bundle-Ether 3
```

(Optional) Shows detailed information about LACP ports and their peers.

Configuring VLAN Bundles

This section describes how to configure a VLAN bundle. The creation of a VLAN bundle involves three main tasks:

1. Create an Ethernet bundle.
2. Create VLAN subinterfaces and assign them to the Ethernet bundle.

3. Assign Ethernet links to the Ethernet bundle.

These tasks are describe in detail in the procedure that follows.

Note In order for a VLAN bundle to be active, you must perform the same configuration on both ends of the bundle connection.

Note Bundled interfaces are supported only in L2transport mode.

The creation of a VLAN link bundle is described in the steps that follow.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters XR Config mode.

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname#(config)# interface Bundle-Ether 3
```

Creates and names a new Ethernet link bundle.

This **interface Bundle-Ether** command enters you into the interface configuration submode, where you can enter interface specific configuration commands are entered. Use the **exit** command to exit from the interface configuration submode back to the normal XR Config mode.

Step 3 **bundle minimum-active bandwidth** *kbps*

Example:

```
RP/0/RP0:hostname(config-if) # bundle minimum-active bandwidth 580000
```

(Optional) Sets the minimum amount of bandwidth required before a user can bring up a bundle.

Step 4 **bundle minimum-active links** *links*

Example:

```
RP/0/RP0:hostname(config-if)# bundle minimum-active links 2
```

(Optional) Sets the number of active links required before you can bring up a specific bundle.

Step 5 **bundle maximum-active links** *links*

Example:

```
RP/0/RP0:hostname(config-if)# bundle maximum-active links 1
```

(Optional) Designates one active link and one link in standby mode that can take over immediately for a bundle if the active link fails (1:1 protection).

Note The default number of active links allowed in a single bundle is 8.

Note If the **bundle maximum-active** command is issued, then only the highest-priority link within the bundle is active. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, we recommend that you configure a higher priority on the link that you want to be the active link.

Step 6 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration submode.

Step 7 **interface Bundle-Ether** *bundle-id.vlan-id* **l2transport**

Example:

```
RP/0/RP0:hostname#(config)#interface Bundle-Ether 3.1 l2transport
```

Creates a new VLAN, and assigns the VLAN to the Ethernet bundle you created in Step 2.

Replace the *bundle-id* argument with the *bundle-id* you created in Step 2.

Replace the *vlan-id* with a subinterface identifier.

Note When you include the *vlan-id* argument with the **interface Bundle-Ether** *bundle-id* command, you enter subinterface configuration mode.

Step 8 **encapsulation dot1q** *vlan-id*

Example:

```
RP/0/RP0:hostname#(config-subif)# encapsulation dot1q 10
```

Assigns a VLAN to the subinterface.

Replace the *vlan-id* argument with a subinterface identifier.

Step 9 **no shutdown**

Example:

```
RP/0/RP0:hostname(config-subif) # no shutdown
```

(Optional) If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up state.

Step 10 **exit**

Example:

```
RP/0/RP0:hostname(config-subif)#exit
```

Exits subinterface configuration mode for the VLAN subinterface.

Step 11 Repeat Step 7 through Step 12 to add more VLANs to the bundle you created in Step 2.

(Optional) Adds more subinterfaces to the bundle.

Step 12 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Step 13 **exit**

Example:

```
RP/0/RP0:hostname (config-subif)# exit
```

Exits interface configuration mode.

Step 14 **exit**

Example:

```
RP/0/RP0:hostname (config)# exit
```

Exits XR Config mode.

Step 15 **show ethernet trunk bundle-Ether** *instance*

Example:

```
RP/0/RP0:hostnamerouter# show ethernet trunk bundle-ether 5
```

(Optional) Displays the interface configuration.

The Ethernet bundle instance range is from 1 through 65535.

Step 16 **configure**

Example:

```
RP/0/RP0:hostname#  configure
```

Enters XR Config mode.

Step 17 **interface** { **GigabitEthernet** | **HundredGigabitE** } *instance*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 1/0/0/0
```

Enters the interface configuration mode for the specified interface.

Replace the *instance* argument with the node-id in the *rack/slot/module* format.

Note A VLAN bundle is not active until you add an Ethernet interface on both ends of the link bundle.

Step 18 **bundle id** `bundle-id` **[mode {active | on | passive}]**

Example:

```
RP/0/RP0:hostname(config-if)#  bundle-id 3
```

Adds an Ethernet interface to the bundle you configured in Step 2 through Step 13.

To enable active or passive LACP on the bundle, include the optional **mode active** or **mode passive** keywords in the command string.

To add the interface to the bundle without LACP support, include the optional **mode on** keywords with the command string.

Note If you do not specify the **mode** keyword, the default mode is **on** (LACP is not run over the port).

Step 19 **no shutdown**

Example:

```
RP/0/RP0:hostname(config-if)# no shutdown
```

(Optional) If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up or down state depending on the configuration and state of the link.

Step 20 Repeat Step 19 through Step 21 to add more Ethernet interfaces to the bundle you created in Step 2 .

Step 21 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Step 22 Perform Step 1 through Step 23 on the remote end of the connection.

Brings up the other end of the link bundle.

Step 23 **show bundle Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname#show bundle Bundle-Ether 3
```

(Optional) Shows information about the specified Ethernet link bundle.

The **show bundle Bundle-Ether** command displays information about the specified bundle. If your bundle has been configured properly and is carrying traffic, the State field in the **show bundle Bundle-Ether** command output will show the number “4,” which means the specified VLAN bundle port is “distributing.”

Step 24 **show ethernet trunk bundle-Ether** *instance*

Example:

```
RP/0/RP0:hostname# show ethernet trunk bundle-ether 5
```

(Optional) Displays the interface configuration.

The Ethernet bundle instance range is from 1 through 65535.

Configuring L3 Ethernet Link Bundles

This section describes how to configure a Layer 3 Ethernet link bundle.

Note In order for an Ethernet bundle to be active, you must perform the same configuration on both connection endpoints of the bundle.

The creation of an Ethernet link bundle involves creating a bundle and adding member interfaces to that bundle, as shown in the steps that follow.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the XR Config mode.

Step 2 **interface Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname(config)# interface Bundle-Ether 3
```

Creates and names a new Ethernet link bundle.

Step 3 **ipv4 address** *ipv4-address mask*

Sets the IP address and mask.

Step 4 **bundle minimum-active bandwidth** *kbps*

Example:

```
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 580000
```

(Optional) Sets the minimum amount of bandwidth required before a user can bring up a bundle.

Step 5 **bundle minimum-active links** *links*

Example:

```
RP/0/RP0:hostname(config-if)# bundle minimum-active links 2
```

(Optional) Sets the number of active links required before you can bring up a specific bundle.

Step 6 **bundle maximum-active links** *links*

Example:

```
RP/0/RP0:hostname(config-if)# bundle maximum-active links 1
```

(Optional) Designates one active link and one link in standby mode that can take over immediately for a bundle if the active link fails (1:1 protection).

The default number of active links in a single bundle is 8.

Note If the **bundle maximum-active** command is issued, then only the highest-priority link within the bundle is active. The priority is based on the value from the **bundle port-priority** command, where a lower value is a higher priority. Therefore, we recommend that you configure a higher priority on the link that you want to be the active link.

Step 7 **bundle maximum-active links** *links* **hot-standby**

Example:

```
RP/0/RP0:hostname(config-if)# bundle maximum-active links 1 hot-standby
```

The **hot-standby** keyword helps to avoid bundle flaps on a switchover or switchback event during which the bundle temporarily falls below the minimum links or bandwidth threshold.

It sets default values for the wait-while timer and suppress-flaps timer to achieve this.

Step 8 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration submode for the Ethernet link bundle.

Step 9 **interface** { **TenGigE** | **HundredGigE** | **FortyGigE** } *instance*

Example:

```
RP/0/RP0:hostname(config)# interface fortyGigE 0/6/0/4
```

Enters the interface configuration mode for the specified interface.

Mixed bandwidth bundle member configuration is only supported when 1:1 redundancy is configured.

Note Mixed link bundle mode is supported only when active-standby operation is configured (usually with the lower speed link in standby mode).

Step 10 **bundle id** *bundle-id* [**mode** { **active** | **on** | **passive**}]

Example:

```
RP/0/RP0:hostname(config-if)# bundle-id 3
```

Adds the link to the specified bundle.

Note If you do not specify the **mode** keyword, the default mode is **on**

Step 11 **no shutdown**(optional)

Example:

```
RP/0/RP0:hostname(config-if)# no shutdown
```

If a link is in the down state, bring it up. The **no shutdown** command returns the link to an up or down state depending on the configuration and state of the link.

Step 12 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration submode for the Ethernet link bundle.

Step 13 Repeat Step 8 through Step 11 to add more links to the bundle you created in Step 2.

Step 14 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Step 15 **exit**

Example:

```
RP/0/RP0:hostname(config-if)# exit
```

Exits interface configuration mode.

Step 16 **exit**

Example:

```
RP/0/RP0:hostname(config)# exit
```

Exits the XR Config mode.

Step 17 Perform Step 1 through Step 15 on the remote end of the connection.

Brings up the other end of the link bundle.

Step 18 **show bundle Bundle-Ether** *bundle-id* [**reasons**] (optional)

Example:

```
RP/0/RP0:hostname# show bundle Bundle-Ether 3 reasons
```

Shows information about the specified Ethernet link bundle

Step 19 **show lacp Bundle-Ether** *bundle-id*

Example:

```
RP/0/RP0:hostname # show lacp Bundle-Ether 3
```

(Optional) Shows detailed information about LACP ports and their peers.

Example

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# ipv4 address 100.110.100.2/24
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 620000
RP/0/RP0:hostname(config-if)# bundle minimum-active links 1
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface FortyGigE 0/6/0/4
RP/0/RP0:hostname(config-if)# bundle id 3 mode active
RP/0/RP0:hostname(config-if)# no shutdown
RP/0/RP0:hostname(config)# exit
RP/0/RP0:hostname(config)# interface FortyGigE 0/6/0/9
RP/0/RP0:hostname(config-if)# bundle id 3 mode active
RP/0/RP0:hostname(config-if)# no shutdown
RP/0/RP0:hostname(config-if)# exit
```

Configuration Examples for Link Bundles

Configuring Ethernet Channel Bundle with LACP mode: Example

This example shows how to join two ports to form an Ethernet Channel bundle running LACP:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 3
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 620000
RP/0/RP0:hostname(config-if)# bundle minimum-active links 1
RP/0/RP0:hostname(config-if)# l2transport
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 3
RP/0/RP0:hostname(config)# interface TenGigE 0/3/0/0
RP/0/RP0:hostname(config-if)# bundle id 3 mode active
RP/0/RP0:hostname(config-if)# no shutdown
RP/0/RP0:hostname(config)# exit
RP/0/RP0:hostname(config)# interface TenGigE 0/3/0/1
RP/0/RP0:hostname(config-if)# bundle id 3 mode active
RP/0/RP0:hostname(config-if)# no shutdown
RP/0/RP0:hostname(config-if-l2)# exit
```

Configuring Ethernet Channel Bundle with Non LACP or Static Mode : Example

This example shows how to join two ports to form an Ethernet Channel bundle with non-LACP/static mode :

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 2002
RP/0/RP0:hostname(config-if)# bundle minimum-active links 1
RP/0/RP0:hostname(config-if)# l2transport
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface TenGigE0/2/0/9/4
RP/0/RP0:hostname(config-if)# bundle id 2002 mode on
RP/0/RP0:hostname(config-if)# no shutdown
RP/0/RP0:hostname(config)# exit
```

```
RP/0/RP0:hostname(config)# interface TenGigE0/3/0/9/4
RP/0/RP0:hostname(config-if)# bundle id 2002 mode on
RP/0/RP0:hostname(config-if)# no shutdown
RP/0/RP0:hostname(config)# exit
```

Creating VLAN Subinterface on a Ethernet Bundle: Example

This example shows how to create and bring up two VLANs on an Ethernet bundle:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 620000
RP/0/RP0:hostname(config-if)# bundle minimum-active links 1
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
RP/0/RP0:hostname(config-subif)# no shutdown
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 1.2 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 20
RP/0/RP0:hostname(config-subif)# no shutdown
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)#interface tengige 0/1/5/7
RP/0/RP0:hostname(config-if)# bundle-id 1 mode act
RP/0/RP0:hostname(config-if)# commit
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# exit
RP/0/RP0:hostname # show ethernet trunk bundle-ether 1
```

Configure L2VPN with Ethernet Bundle as Attachment Circuit : Examples

Following example shows how to configure local switching with bundled interface:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface TenGigE0/0/0/2
RP/0/RP0:hostname(config-if)# bundle-id 1 mode on
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 2
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 2.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface TenGigE0/5/0/7
RP/0/RP0:hostname(config-if)# bundle-id 2 mode on
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)#controller Optics 0/0/0/2
RP/0/RP0:hostname(config-Optics)# port-mode Ethernet framing packet rate 10GE
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)#controller Optics 0/5/0/7
RP/0/RP0:hostname(config-Optics)# port-mode Ethernet framing packet rate 10GE
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group XCON2
```

```
RP/0/RP0:hostname(config-l2vpn-xc)# p2p xc2
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether 1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether 2.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# commit
```

Following example shows how to configure dynamic point-to-point cross-connect with bundled interface:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 620000
RP/0/RP0:hostname(config-if)# bundle minimum-active links 1
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
RP/0/RP0:hostname(config-subif)# no shutdown
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface tengige0/1/5/7
RP/0/RP0:hostname(config-if)# bundle-id 1 mode on
RP/0/RP0:hostname(config-if)# commit
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# pw-class dyn-mpls
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)# ipv4 source 106.0.0.1
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)# preferred-path interface tunnel-te 1
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)# exit
RP/0/RP0:hostname(config-l2vpn-pwc)# exit
RP/0/RP0:hostname(config-l2vpn)# xconnect group XCON1
RP/0/RP0:hostname(config-l2vpn-xc)# p2p xc1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether 1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor ipv4 107.0.0.1 pw-id 1
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class dyn-mpls
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# commit
```

Configure CFM with Ethernet Bundle: Examples

Note The possible intervals for transmitting Continuity Check Messages (CCMs), that can be used with bundles are : 1s, 10s, 1m ,and 10s.

Note For more details on CFM refer section .

Example1:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
RP/0/RP0:hostname(config-subif)# ethernet cfm mep domain d1 service s1 mep-id 1
RP/0/RP0:hostname(config-if-cfm-mep)# exit
```

```
RP/0/RP0:hostname(config-if-cfm)# exit
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface TenGigE0/0/0/2
RP/0/RP0:hostname(config-if)# bundle-id 1 mode on
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 2
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 2.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
RP/0/RP0:hostname(config-subif)# ethernet cfm mep domain d2 service s2 mep-id 2
RP/0/RP0:hostname(config-if-cfm-mep)# exit
RP/0/RP0:hostname(config-if-cfm)# exit
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface TenGigE0/5/0/7
RP/0/RP0:hostname(config-if)# bundle-id 2 mode on
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)#controller Optics 0/0/0/2
RP/0/RP0:hostname(config-Optics)# port-mode Ethernet framing packet rate 10GE
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)#controller Optics 0/5/0/7
RP/0/RP0:hostname(config-Optics)# port-mode Ethernet framing packet rate 10GE
RP/0/RP0:hostname(config-if)# exit

RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group XCON2
RP/0/RP0:hostname(config-l2vpn-xc)# p2p xc2
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether 1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether 2.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# commit
```

Example2:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface Bundle-Ether 1
RP/0/RP0:hostname(config-if)# bundle minimum-active bandwidth 620000
RP/0/RP0:hostname(config-if)# bundle minimum-active links 1
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether 1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 10
RP/0/RP0:hostname(config-subif)# ethernet cfm mep domain d1 service s1 mep-id 1
RP/0/RP0:hostname(config-if-cfm-mep)# exit
RP/0/RP0:hostname(config-if-cfm)# exit
RP/0/RP0:hostname(config-subif)# no shutdown
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# interface tengige0/1/5/7
RP/0/RP0:hostname(config-if)# bundle-id 1 mode on
RP/0/RP0:hostname(config-if)# commit
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# pw-class dyn-mpls
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)# ipv4 source 106.0.0.1
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)# preferred-path interface tunnel-te 1
RP/0/RP0:hostname(config-l2vpn-pwc-mpls)# exit
RP/0/RP0:hostname(config-l2vpn-pwc)# exit
RP/0/RP0:hostname(config-l2vpn)# xconnect group XCON1
RP/0/RP0:hostname(config-l2vpn-xc)# p2p xc1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether 1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor ipv4 107.0.0.1 pw-id 1
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class dyn-mpls
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# commit
```

Configure AIS for CFM with Ethernet Bundle: Examples

Note The possible intervals for transmitting Continuity Check Messages (CCMs), that can be used with bundles are : 1s, 10s, 1m ,and 10s.

Example1:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)#ethernet cfm
RP/0/RP0:hostname(config-cfm)#domain dup3 level 3 id null
RP/0/RP0:hostname(config-cfm-dmn)#service sup3 down-meps id icc-based cisco u3
RP/0/RP0:hostname(config-cfm-dmn-svc)#continuity-check interval 1s
RP/0/RP0:hostname(config-cfm-dmn-svc)#mep crosscheck
RP/0/RP0:hostname(config-cfm-xcheck)#mep-id 3
RP/0/RP0:hostname(config-cfm-xcheck)#exit
RP/0/RP0:hostname(config-cfm-dmn-svc)#ais transmission
RP/0/RP0:hostname(config-cfm-dmn-svc)#exit
```

Example2:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)#ethernet cfm
RP/0/RP0:hostname(config-cfm)#domain dup4 level 4 id null
RP/0/RP0:hostname(config-cfm-dmn)#service sup3 xconnect group arw-g3 p2p arw_p3$
RP/0/RP0:hostname(config-cfm-dmn-svc)#mip auto-create all
RP/0/RP0:hostname(config-cfm-dmn-svc)#continuity-check interval 1s
RP/0/RP0:hostname(config-cfm-dmn-svc)#mep crosscheck
RP/0/RP0:hostname(config-cfm-xcheck)#mep-id 3
RP/0/RP0:hostname(config-cfm-xcheck)#exit
RP/0/RP0:hostname(config-cfm-dmn-svc)#ais transmission
RP/0/RP0:hostname(config-cfm-dmn-svc)#exit
```

Ethernet CFM Show Command for Ethernet Bundle: Examples

Example1:

```
RP/0/RP0:hostname# show ethernet cfm local meps interface bundle-Ether 1.3
Thu Sep 20 22:53:01.969 UTC
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
C - Config (our ID received)    M - Missing (cross-check)
X - Cross-connect (wrong MAID)  U - Unexpected (cross-check)
P - Peer port down

Domain dup3 (level 3), Service sup3
   ID Interface (State)        Dir MEPs/Err RD Defects AIS
----- ----------------------- --- -------- -- ------- ---
3003 BE1.3 (Up)               Dn     0/0   Y  TM      L4
```

Example 2:

```
RP/0/RP0:hostname# show ethernet cfm peer meps
Thu Sep 20 22:53:36.337 UTC
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    S - Standby

Domain MD1 (level 1), Service down_mep_customer_20001
Down MEP on Bundle-Ether2000.1 MEP-ID 6001
================================================================================
St    ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
>  7001 00af.1fd6.0021 Up      00:01:56          136     0     0     0
Domain MD1 (level 1), Service down_mep_customer_20002

Down MEP on Bundle-Ether2000.2 MEP-ID 6002
================================================================================
St    ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
>  7002 00af.1fd6.0021 Up      00:01:56          139     0     0     0
Domain MD2 (level 2), Service up_mep_customer_1001
Up MEP on Bundle-Ether2000.1 MEP-ID 4001
================================================================================
St    ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
>  5501 7ef2.fe69.3123 Up      00:01:01           62      0     0     0

Domain MD2 (level 2), Service up_mep_customer_1002
Up MEP on Bundle-Ether2000.2 MEP-ID 4002
================================================================================
St    ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
>  5502 7ef2.fe69.3123 Up      00:01:01           62      0     0     0
```

Example 3:

```
RP/0/RP0:hostname# show ethernet cfm peer meps interface bundle-Ether 1.3 detail
Thu Sep 20 22:53:52.899 UTC
Domain dup3 (level 3), Service sup3
Down MEP on Bundle-Ether1.3 MEP-ID 3003
================================================================================
Peer MEP-ID 3, MAC 92bd.4a00.0023
   CFM state: Timed out, for 00:01:50
   Port state: Up
   CCM defects detected:    T - Timed out
   CCMs received: 1673
     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 00:01:53 ago:
     Level: 3, Version: 0, Interval: 1s
     Sequence number: 0, MEP-ID: 3
     MAID: NULL, ICC-based: ciscou3
     Chassis ID: Local: ios; Management address: 'Not specified'
     Port status: Up, Interface status: Up
```

```
Peer MEP-ID 3, MAC
   CFM state: Missing (cross-check), no CCMs received
   CCM defects detected:    M - Missing (cross-check)
   CCMs received: 0
     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
```

Example 4:

```
RP/0/RP0:hostname# show ethernet cfm local meps interface bundle-Ether 1.3 verbose
Thu Sep 20 22:55:18.149 UTC
Domain dup3 (level 3), Service sup3
Down MEP on Bundle-Ether1.3 MEP-ID 3003
================================================================================
  Interface state: Up      MAC address: 4481.9800.0023
  Peer MEPs: 0 up, 0 with errors, 1 timed out (archived)
  Cross-check errors: 1 missing, 0 unexpected

  CCM generation enabled:  Yes, 1s (Remote Defect detected: Yes)
  CCM defects detected:    T - Timed out
                           M - Missing (cross-check)
  AIS generation enabled:  Yes (level: 4, interval: 1s)
  Sending AIS:             Yes (started 00:03:15 ago)
  Receiving AIS:           No

  Packet        Sent      Received
  ------  ----------  ----------------------------------------------------------
  CCM           6594          1673  (out of seq: 0)
  AIS            196             0
```

Example 5:

```
RP/0/RP0:hostname# show ethernet cfm interfaces ais
Thu Sep 20 22:52:10.824 UTC
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
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
------------------------ ---  - -------  -------  - ----- ------------ --------
BE1.3 (Up)               Up   3 TM                4 1s    00:00:08 ago        9
```

Configuring ISIS for L3 Link Bundle : Example

This example shows how to configure ISIS for layer3 link bundles:

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)#router isis 100
```

```
RP/0/RP0:hostname(config-isis)#instance-id 789
RP/0/RP0:hostname(config-isis)#interface bundle-ether 1
RP/0/RP0:hostname(config-isis-if)#address-family ipv4 unicast
RP/0/RP0:hostname(config-isis-if-af)# commit
```

Show Command for L3 Ethernet Bundle: Examples

Example1:

```
RP/0/RP0:hostname# show bundle bundle-ether 1
Thu Sep  6 08:31:06.471 UTC

Bundle-Ether1
  Status:                                    Up
  Local links <active/standby/configured>:   2 / 0 / 2
  Local bandwidth <effective/available>:     80000000 (80000000) kbps
  MAC address (source):                      5a79.5b00.0023 (Chassis pool)
  Inter-chassis link:                        No
  Minimum active links / bandwidth:          1 / 1 kbps
  Maximum active links:                      16
  Wait while timer:                          2000 ms
  Load balancing:
    Link order signaling:                    Not configured
    Hash type:                               Default
    Locality threshold:                      None
  LACP:                                      Operational
    Flap suppression timer:                  Off
    Cisco extensions:                        Disabled
    Non-revertive:                           Disabled
  mLACP:                                     Not configured
  IPv4 BFD:                                  Not configured
  IPv6 BFD:                                  Not configured

  Port                  Device           State        Port ID         B/W, kbps
  --------------------  ---------------  -----------  --------------  ----------
  Fo0/6/0/4             Local            Active       0x8000, 0x0001    40000000
      Link is Active
  Fo0/6/0/9             Local            Active       0x8000, 0x0002    40000000
      Link is Active
```

Example 2:

```
RP/0/RP0:hostname# show arp bundle-Ether 1 location 0/lc0
Thu Sep  6 08:31:32.032 UTC

Address         Age        Hardware Addr   State      Type  Interface
100.110.100.2   -          5a79.5b00.0023  Interface  ARPA  Bundle-Ether1
RP/0/RP0:KK05#show arp bundle-Ether 1 location 0/lc0
Thu Sep  6 08:31:53.523 UTC

Address         Age        Hardware Addr   State      Type  Interface
100.110.100.1   00:00:07   5a79.5d00.0023  Dynamic    ARPA  Bundle-Ether1
100.110.100.2   -          5a79.5b00.0023  Interface  ARPA  Bundle-Ether1
```

Example 3:

```
RP/0/RP0:hostname# show isis neighbors
Thu Sep  6 08:32:37.399 UTC

IS-IS 100 neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
```

```
MM10           BE1              5a79.5d00.0023 Up    8        L1L2 Capable
IORNMAN-BACKUP Te0/6/0/7/1      b026.803a.3011 Up    9        L1L2 Capable

Total neighbor count: 2

IS-IS jkcore neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
0000.0000.0004 Te0/6/0/5/1      a80c.0d7b.f7aa Up    8        L2   Capable

Total neighbor count: 1
```

CHAPTER 49

Configure Link Layer Discovery Protocol

Table 51: Feature History

Feature Name	Release Information	Description
Link Layer Discovery Protocol (LLDP) on NCS4K-4H-OPW-QC2 line card	Cisco IOS XR Release 6.5.33	In addition to the existing support on packet interfaces, Link Layer Discovery Protocol (LLDP) is now enabled on the client ports of the NCS4K-4H-OPW-QC2 card that carry Ethernet-over-OTN traffic. This feature allows NCS 4000 to discover peer devices connected either on the OTN ports or the packet interfaces. As a result, it reduces the need to use multiple protocols for network management, especially in a multi-vendor network. Commands added: • show lldp neighbors • show lldp neighbors detail

This chapter describes the procedures to configure Link Layer Discovery Protocol on Cisco NCS 4000 Series routers using CLI.

Link Layer Discovery Protocol (LLDP) - Overview

To support non-Cisco devices and to allow for interoperability between other devices, the Cisco NCS 4000 Series Router supports the IEEE 802.1AB LLDP. LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol also allows NCS 4000 devices to discover information about its peer devices connected through the OTN ports and the packet interfaces. This protocol runs over the Data Link Layer, which allows two systems running different network layer protocols to learn about each other. The feature is supported on client ports of the NCS4K-4H-OPW-QC2 card that support Ethernet-over-OTN configuration and the packet interfaces.

LLDP supports a set of attributes that it uses to learn information about neighbor devices. These attributes have a defined format known as a Type-Length-Value (TLV). LLDP supported devices can use TLVs to receive and send information to their neighbors. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.

In addition to the mandatory TLVs (Chassis ID, Port ID, and Time-to-Live), the router also supports the following basic management TLVs, which are optional:

- Port Description
- System Name
- System Description
- System Capabilities
- Management Address

These optional TLVs are automatically sent when LLDP is active, but you can disable them as needed using the lldp tlv-select disable command.

LLDP Frame Format

LLDP frames use the IEEE 802.3 format, which consists of the following fields:

- Destination address (6 bytes)—Uses a multicast address of 01-80-C2-00-00-0E.
- Source address (6 bytes)—MAC address of the sending device or port.
- LLDP Ethertype (2 bytes)—Uses 88-CC.
- LLDP PDU (1500 bytes)—LLDP payload consisting of TLVs.
- FCS (4 bytes)—Cyclic Redundancy Check (CRC) for error checking.

LLDP TLV Format

LLDP TLVs carry the information about neighboring devices within the LLDP PDU using the following basic format:

- TLV Header (16 bits), which includes the following fields:
  - TLV Type (7 bits)

    - TLV Information String Length (9 bits)

- TLV Information String (0 to 511 bytes)

LLDP Operation

LLDP is a one-way protocol. The basic operation of LLDP consists of a device enabled for transmit of LLDP information sending periodic advertisements of information in LLDP frames to a receiving device.

Devices are identified using a combination of the Chassis ID and Port ID TLVs to create an MSAP (MAC Service Access Point). The receiving device saves the information about a neighbor for a certain amount time specified in the TTL TLV, before aging and removing the information.

LLDP supports the following additional operational characteristics:

- LLDP can operate independently in transmit or receive modes.
- LLDP operates as a slow protocol using only untagged frames, with transmission speeds of less than 5 frames per second.
- LLDP packets are sent when the following occurs:
    - The packet update frequency specified by the lldp timer command is reached. The default is 30 seconds.
    - When a change in the values of the managed objects occurs from the local system's LLDP MIB.
    - When LLDP is activated on an interface (3 frames are sent upon activation).
- When an LLDP frame is received, the LLDP remote services and PTOPO MIBs are updated with the information in the TLVs.
- LLDP supports the following actions on these TLV characteristics:
    - Interprets a TTL value of 0 as a request to automatically purge the information of the transmitting device. These shutdown LLDPDUs are typically sent prior to a port becoming inoperable.
    - An LLDP frame with a malformed mandatory TLV is dropped.
    - A TLV with an invalid value is ignored.
    - A copy of an unknown organizationally-specific TLV is maintained if the TTL is non-zero, for later access through network management.

Supported LLDP Functions

The Cisco NCS 4000 Series Router supports the following LLDP functions:

- IPv4 management addresses—In general, IPv4 addresses will be advertised if they are available, and preference is given to the address that is configured on the transmitting interface.

If the transmitting interface does not have a configured address, then the TLV will be populated with an address from another interface. The advertised LLDP IP address is implemented according to the following priority order of IP addresses for interfaces on the Cisco NCS 4000 Series Router:

- Locally configured address
- MgmtEth0/RP0/CPU0/0
- MgmtEth0/RP0/CPU0/1
- MgmtEth0/RP1/CPU0/0
- MgmtEth0/RP1/CPU0/1
- Loopback interfaces

- LLDP is supported for the nearest physically attached, non-tunneled neighbors.
- Port ID TLVs are supported for Ethernet interfaces, subinterfaces, bundle interfaces, and bundle subinterfaces.

Unsupported LLDP Functions

The following LLDP functions are not supported on the Cisco NCS 4000 Series Router:

- LLDP-MED organizationally unique extension—However, interoperability still exists between other devices that do support this extension.
- Tunneled neighbors, or neighbors more than one hop away.
- LLDP TLVs cannot be disabled on a per-interface basis; However, certain optional TLVs can be disabled globally.
- LLDP SNMP trap lldpRemTablesChange.

Configuring LLDP

This section includes the procedures for configuring LLDP.

LLDP Default Configuration

Table below shows the values of the LLDP default configuration on the Cisco NCS 4000 Series Router. To change the default settings, use the LLDP global configuration and LLDP interface configuration commands.

Table 52: LLDP Default Configuration

LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds

LLDP reinitialization delay	2 seconds
LLDP TLV selection	All TLVs are enabled for sending and receiving.
LLDP interface state	Enabled for both transmit and receive operation when LLDP is globally enabled.

Enabling LLDP Globally

To run LLDP on the router, you must enable it globally. When you enable LLDP globally, all interfaces that support LLDP are automatically enabled for both transmit and receive operations.

You can override this default operation at the interface to disable receive or transmit operations. For more information about how to selectively disable LLDP receive or transmit operations for an interface, see the "Disabling LLDP Receive and Transmit Operation for an Interface" section.

To enable LLDP globally, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the XR Config mode.

Step 2 **lldp**

Example:

```
RP/0/RP0:hostname(config)# lldp
```

Enables LLDP globally for both transmit and receive operation on the system.

Step 3 Use the **commit** or **end** command.

Example:

```
RP/0/RP0:hostname(config-lldp)# commit
```

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring Global LLDP Operational Characteristics

The "LLDP Default Configuration" section describes the default operational characteristics for LLDP. When you enable LLDP globally on the router using the lldp command, these defaults are used for the protocol.

To modify the global LLDP operational characteristics such as the LLDP neighbor information holdtime, initialization delay, or packet rate, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the XR Config mode.

Step 2 **lldp holdtime** *time -in-seconds*

Example:

```
RP/0/RP0:hostname(config)# lldp holdtime 60
```

(Optional) Specifies the length of time that information from an LLDP packet should be held by the receiving device before aging and removing it.

Step 3 **lldp reinit** *time -in-seconds*

Example:

```
RP/0/RP0:hostname(config)# lldp reinit 4
```

(Optional) Specifies the length of time to delay initialization of LLDP on an interface.

Step 4 **lldp timer** *time -in-seconds*

Example:

```
RP/0/RP0:hostname(config)# lldp timer 60
```

(Optional) Specifies the LLDP packet rate.

Step 5 Use the **commit** or **end** command.

Example:

```
RP/0/RP0:hostname(config)# commit
```

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.

- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Disabling Transmission of Optional LLDP TLVs

Certain TLVs are classified as mandatory in LLDP packets, such as the Chassis ID, Port ID, and Time to Live (TTL) TLVs. These TLVs must be present in every LLDP packet. You can suppress transmission of certain other optional TLVs in LLDP packets.

To disable transmission of optional LLDP TLVs, complete the following steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the XR Config mode.

Step 2 **lldp tlv-select** *tlv-name* **disable**

Example:

```
RP/0/RP0:hostname(config)# lldp tlv-select system-capabilities disable
```

(Optional) Specifies that transmission of the selected TLV in LLDP packets is disabled. The tlv-name can be one of the following LLDP TLV types:

- management-address
- port-description
- system-capabilities
- system-description
- system-name

Step 3 Use the **commit** or **end** command.

Example:

```
RP/0/RP0:hostname(config)# commit
```

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Disabling LLDP Receive and Transmit Operation for an Interface

When you enable LLDP globally on the router, all supported interfaces are automatically enabled for LLDP receive and transmit operation. You can override this default by disabling these operations for a particular interface.

To disable LLDP receive and transmit operations for an interface, complete the following steps:

-

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0:hostname# configure
```

Enters the XR Config mode.

Step 2 **interface** [**TenGigE** | **HundredGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname(config)# interface TenGigE 0/6/0/2
```

Enters interface configuration mode and specifies the Ethernet interface name and notation rack/slot/module/port. Possible interface types for this procedure are:

- TenGigE
- HundredGigE

Step 3 **lldp**

Example:

```
RP/0/RP0:hostname(config-if)# lldp
```

(Optional) Enters LLDP configuration mode for the specified interface.

Step 4 **receive disable**

Example:

```
RP/0/RP0:hostname(config-if-lldp)# receive disable
```

(Optional) Disables LLDP receive operations on the interface.

Step 5 **transmit disable**

Example:

```
RP/0/RP0:hostname(config-if-lldp)# transmit disable
```

(Optional) Disables LLDP transmit operations on the interface.

Step 6 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Verifying the LLDP Configuration

This section describes how you can verify the LLDP configuration both globally and for a particular interface.

Procedure

Step 1 **show lldp**

Example:

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

Displays the LLDP global configuration status and operational characteristics.

```
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
```

Step 2 **show lldp interface** [**TenGigE** | **HundredGigE**] *interface-path-id*

Example:

```
RP/0/RP0:hostname# show lldp interface TenGigE 0/1/0/7
```

Displays the LLDP interface status and configuration.

```
Wed Dec 13 13:22:30.501 DST
TenGigE0/1/0/7:
        Tx: enabled
        Rx: enabled
        Tx state: IDLE
        Rx state: WAIT FOR FRAME
```

View the Neighbor Device Details Using CLI

You can view details of the neighbor devices connected to NCS 4000 using the **show lldp neighbors** and **show lldp neighbors detail** commands.

Procedure

Issue one of the following:

a) **show lldp neighbors**

b) **show lldp neighbors detail**

For more details about these commands, see the Link Layer Discovery Protocol (LLDP) Command Reference section of Command Reference for Cisco NCS 4000 Series guide.

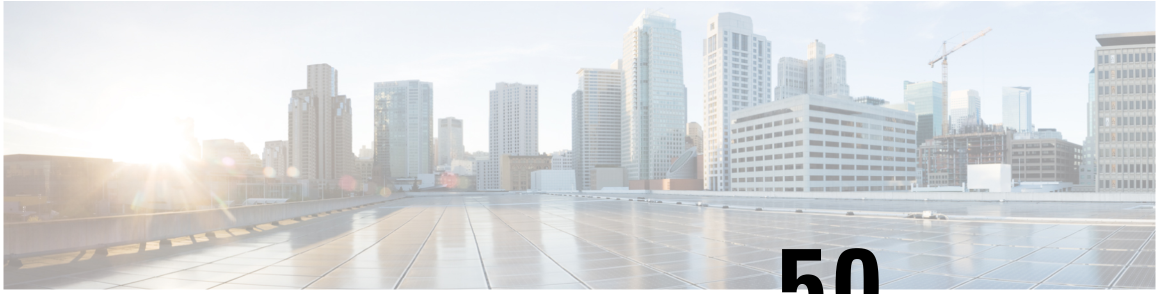
Examples

The following example shows how to view the neighbor devices connected to NCS 4000:

```
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
[DISABLED] TenGigECtrlr0/5/0/4/1 17 N/A

Total entries displayed: 1
```

The following example shows how to view the neighbor device details connected to NCS 4000:

```
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
```



CHAPTER 50

Configure Affinity for OTN

This chapter describes the XR procedure for configuring Affinity Support for OTN GMPLS.

Configuring Affinity for GMPLS using Cisco IOS XR commands

Procedure

Step 1 Define colours and assign bits to each colour using command : **affinity-map** <*colour*> **bit-position** <*bit position*>

Example:

```
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-mpls-te)# affinity-map green bit-position 0
```

Note Only one colour can be mapped to a particular bit position.

Note Same bit map should defined at all the connected nodes.

Step 2 Assign one or multiple colours to the OTN link using command **affinity-name**<*colour*>

Example:

```
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
```

Note Assign colour to all the ports of the connected nodes.

Step 3 Define an attribute set using command **attribute-set path-option**

This will define the affinity constraints.

Example:

```
RP/0/RP0:hostname# configure terminal
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
```

Step 4 Configure **attribute-set** for **path–option** for OTN tunnel.

This will assign affinity constraints to OTN tunnel. Following are the constraint type:

- **include** : 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** : 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**: 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.

Note In case of exclude-all constraint, other configured constraints for the same tunnel will be ignored.

Example:

```
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 7
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)# signalled-bandwidth ODU2
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)# destination ipv4 unicast 192.168.0.3
RP/0/RP0:hostname(config-te-gmpls-tun-0x7)# path-option 1 dynamic attribute-set Affinity1
protected-by 2 restored-from 3 lockdown
RP/0/RP0:hostnam (config-te-gmpls-tun-0x7)# path-option 2 dynamic attribute-set Affinity2
lockdown
```

Step 5 Verify the configurations using show commands.

Example:

```
RP/0/RP0:hostname# show mpls traffic-eng affinity-map

Tue Jun 26 15:12:01.948 IST
                      Affinity Name     Bit-position            Affinity Value
Affinity Table
  ----------------------------------   --------------        -----------------------
----------------
                                red               2         0x::4
Mapping
                             yellow               3         0x::8
Mapping
                               blue              21         0x::20:0
Mapping
                              green              31         0x::8000:0
Mapping
```

```
RP/0/RP0:hostname# show mpls traffic-eng link-management optical-nni controller otu2 0/0/0/22
```

```
Tue Nov  7 11:52:51.063 IST
System Information::
NNI OTN Links Count: 3 (Maximum NNI OTN Links Supported 300)
Link Name:: OTU20_0_0_22 (Handle:0x00000170, Addr: V4-Unnum 192.168.0.1 [17])
Link Status         : Up
Link Label Type     : G709_ODU
Physical BW         : OTU2 (10.709Gbps)
Max LSP Bandwidth Per Priority(kbps):
  Priority[0] : 7495557
  Priority[1] : 0
  Priority[2] : 0
  Priority[3] : 0
  Priority[4] : 0
  Priority[5] : 0
  Priority[6] : 0
  Priority[7] : 0
Fixed ODU Capabilities:
     Signal Type       Stages            Flags              Resources
                   1   2   3   4   T S 1.25G 2.5G V L Maximum    Unreserved
                   -   -   -   -   - - ----- ---- - - -------    ----------
   ODU2                            Y Y Y     N    N N 1          0
   ODU0            2               Y Y Y     N    N N 8          6
   ODU1            2               Y Y Y     N    N N 4          3
Flex  ODU Capabilities:
     Signal Type       Stages            Flags                Bandwidth(kbps)
                   1   2   3   4   T S 1.25G 2.5G V L Maximum   Unreserved  Max Lsp
                   -   -   -   -   - - ----- ---- - - --------  ----------  --------
   ODUFlex CBR     2               Y Y Y     N    N N 9995277   7495557     7495557
   ODUFlex GFPFix  2               Y Y Y     N    N N 9995277   7494313     7494313

SRLG Values:1,
TTI Mode            : Section Monitoring
TCM ID              : 0
IGP Neighbor Count  : 1
Flooding Status: (1 area)
IGP Area[1]:: OSPF, ring, 0: Flooded
Remote Link Id:V4-Unnum 192.168.0.2 [16], TE Metric: 1
Delay(Configured/Computed/ToFlood): 0/0/300000 micro-sec
Attributes          :  0x2
Attribute Names     :  red(1)
```

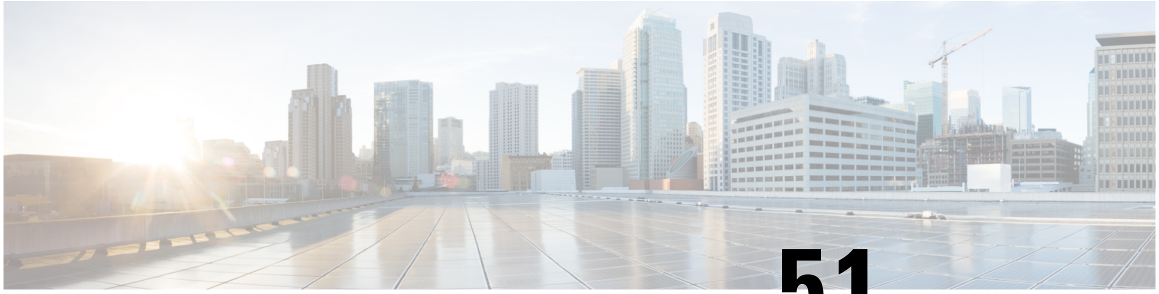
```
RP/0/RP0:hostname# show mpls traffic-eng topology

IGP Id: 192.168.0.4, MPLS TE Id: 192.168.0.4 Router Node  (OSPF ring area 0)
  Link[0]:Point-to-Point, Nbr IGP Id:192.168.0.2, Nbr Node Id:2, gen:28399
      Attribute Flags: 0x2
      Ext Admin Group:
          Length: 256 bits
          Value : 0x::2
     Attribute Names: red(1)
      Intf Id:13 Nbr Intf Id:15 TE Metric:1
      Uni Delay:300000
      SRLGs: 3
      Switching Capability:otn, Encoding:g709-otn
      Physical BW:10709224 (kbps), Max Reservable BW:10709224 (kbps)
      Max LSP Bandwidth Per Priority(kbps):
        Priority[0] : 7495556
        Priority[1] : 0
        Priority[2] : 0
        Priority[3] : 0
        Priority[4] : 0
        Priority[5] : 0
        Priority[6] : 0
        Priority[7] : 0
      Fixed ODU Capabilities:
           Signal Type       Stages           Flags             Resources
                         1   2   3   4   T S 1.25G 2.5G V L Maximum    Unreserved
                         -   -   -   -   - - ----- ---- - - -------    ----------
         ODU2                            Y Y Y     N    N N 1          0
         ODU0            2               Y Y Y     N    N N 8          6
         ODU1            2               Y Y Y     N    N N 4          3
      Flex  ODU Capabilities:
           Signal Type       Stages           Flags               Bandwidth(kbps)

                         1   2   3   4   T S 1.25G 2.5G V L Maximum   Unreserved  Max Lsp

                         -   -   -   -   - - ----- ---- - - --------  ----------  --------

         ODUFlex CBR     2               Y Y Y     N    N N 9995277   7495556     7495556

         ODUFlex GFPFix  2               Y Y Y     N    N N 9995277   7494312     7494312
```

```
RP/0/RP0:hostname# show mpls traffic-eng attribute-set path-option test2

Thu Dec 21 14:12:43.364 IST
Attribute Set Name: test2 (Type: path option)
  Bandwidth: 0 kbps (CT0) (Default)
  Number of affinity constraints: 3
     Include bit map           : 0x2
     Include ext bit map       :
         Length: 256 bits
         Value : 0x::2
     Include affinity name     : red(1)
     Include bit map           : 0x4
     Include ext bit map       :
         Length: 256 bits
         Value : 0x::4
     Include affinity name     : blue(2)
     Include bit map           : 0x8
     Include ext bit map       :
         Length: 256 bits
         Value : 0x::8
     Include affinity name     : yellow(3)
  Exclude List Name:  none (Default)
  List of tunnel IDs (count 0)
```

```
RP/0/RP0:hostname# show mpls traffic-eng tunnels 7 detail

Tue Nov  7 11:19:28.610 IST
Name: Odu-Group-Te7  Destination: 192.168.0.4  Ifhandle:0xd0
  Signalled-Name: rtrA_otn7
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected
    path option 1, (LOCKDOWN) type dynamic  (Basis for Current, path weight 2)
      Protected-by PO index: none
      Path-option attribute: test_red
        Number of affinity constraints: 1
          Include bit map           : 0x2
           Include ext bit map       :
               Length: 256 bits
               Value : 0x::2
           Include affinity name     : red(1)
        Reroute pending (DROP)
```

```
   path option 2, (LOCKDOWN) type dynamic
     Path-option attribute: test_red
       Number of affinity constraints: 1
          Include bit map           : 0x2
          Include ext bit map       :
              Length: 256 bits
              Value : 0x::2
          Include affinity name     : red(1)

   Last PCALC Error [Standby]: Mon Nov  6 16:52:34 2017
     Info: No diverse path found
   Bandwidth Requested: 2498775 kbps  CT0
   Creation Time: Mon Nov  6 15:36:06 2017 (19:43:22 ago)
 Config Parameters:
   Bandwidth: ODU1
   Priority: 24  0 Affinity: 0x0/0xffff
   Metric Type: TE (default)
   Path Selection:
     Tiebreaker: Min-fill (default)
   Hop-limit: disabled
   Cost-limit: disabled
   Delay-limit: disabled
   Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
   AutoRoute: disabled  LockDown:  enabled  Policy class: not set
   Forward class: 0 (not enabled)
   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: 13
 Binding SID: None
 Path Protection Info:
   SNC Mode:SNC-N , TCM id: Not used , Type:Bi-directional APS, Non-revertive
   Restoration style: keep-failed-lsp
   Path Protection Profile Type: 1+0
   Timers WTR: 300000 milliseconds, HoldOff: 0 milliseconds
   Active Lsp: WORKING LSP, Standby Diversity Type: None
 Restoration Info:
   Non-revertive
   Diverse Lsp for UNKNOWN, Diversity Type: None
 Revert Schedule: Not Configured
 Static-uni Info:
   Locally Client Port:   Client Ifhandle: 0x0
   Client ODU:   Client ODU Ifhandle: 0x0
     XC Id: 0
     State: Not Connected
     Uptime: Thu Jan  1 05:30:00 1970
 Working Homepath ERO:
   Status: Down
   Explicit Route:
 Diversity Info:
   Dependent Tunnel List:
      8

 Current LSP Info:
   Instance: 2108, Signaling Area: OSPF ring area 0
   Uptime: 18:27:10 (since Mon Nov 06 16:52:18 IST 2017), Signaling State: Up, Oper State:
Up
   G-PID: None (0)
     XC Id: 0
```

```
      State: Connected
      Uptime: Mon Nov  6 16:52:18 2017
      Egress Interface: OTU20/0/0/22 (State:Up  Ifhandle:0x170)
      Egress Controller: ODU20_0_0_22 (State:Up Ifhandle:0x190)
      Egress Sub Controller: ODU10_0_0_22_41 (State:Up, Ifhandle:0x3d0)
      Path Ingress  label: TPN: 4 BitMap Len: 8 BitMap: 7:8
      Resv Egress  label: TPN: 4 BitMap Len: 8 BitMap: 7:8
    Router-IDs: local      192.168.0.1
                downstream 192.168.0.2
    Soft Preemption: None
    SRLGs: not collected
    Path Info:
      Outgoing:
        Explicit Route:
          Strict, 192.168.0.2(16)
          Strict, 192.168.0.4(13)
          Strict, 192.168.0.4

      Record Route: Empty
      Tspec: signal_type ODU1 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 192.168.0.2, flags 0x20 (Node-ID)
        Label         Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1

        Unnumbered 192.168.0.2 (16), flags 0x0
        Label         Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1
        IPv4 192.168.0.4, flags 0x20 (Node-ID)
        Label         Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1

        Unnumbered 192.168.0.4 (13), flags 0x0
        Label         Label TPN: 4 BitMap Len: 8 BitMap: 7:8 , flags 0x1
      Fspec: signal_type ODU1 Bitrate 0kbps NVC 0 MT 1

  Persistent Forwarding Statistics:
    Out Bytes: 0
    Out Packets: 0
Displayed 1 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```



CHAPTER 51

System Upgrade

On Cisco NCS 4000 routers, system upgrade and package installation processes are executed using **install** commands. The processes involve adding and activating the iso images (.iso), feature packages (.pkg), and software maintenance upgrade files (.smu) on the router. These files are accessed from a network server and then activated on the router. If the installed package or SMU causes any issue on the router, it can be uninstalled.

This chapter provides details of how to upgrade the system using ISSU and OLR.

In-Service Software Upgrade

In-Service Software Upgrade (ISSU) provides the ability to upgrade the router software with no traffic outage. The OTN traffic is hitless whereas packet traffic is impacted.

ISSU is a user-initiated and user-controlled process that uses Cisco nonstop forwarding (NSF) and non-stop routing (NSR). ISSU supports upgrading an image from a lower to a higher version and downgrading an image from a higher version to a lower version.

Processes of ISSU

ISSU on Cisco NCS 4000 enables the Virtual Machines (VM) to run two independent copies of the system software (current version, Version 1; upgraded version, Version 2). The RP VM and the LC VM are upgraded simultaneously. Upgrade using ISSU involves RP switchover and hence two RPs are required.

The upgrade or downgrade using ISSU installation involves:

- Prepare phase—The installable files are pre-checked and loaded on to the router before activation.
- Activate phase—The new image (Version 2) is downloaded to all nodes in the router replacing the old image (Version 1). This phase can be run in step-by-step phases too, such as, Load, Run and Cleanup or by using a one-shot activate phase.
- Commit phase—The ISSU installation is complete with Version 2 on all nodes.

Limitations of ISSU

The limitations of ISSU are:

- Hitless upgrade(s) using ISSU is possible only when the SDKs are compatible. Change in SDK results in the traffic getting affected. OLR is the available solution, see Orchestrated Linecard Reload , on page 727.

  SDK changes are applicable only to packet features and hence OLR is implemented for packet-features; for OTN-only nodes, OLR is not required.

- Multiple simultaneous failures of critical components during an ISSU operation may result in ISSU rollback that will not be hitless.
- Telnet/SSH connectivity will be momentarily lost during switchover to the new software during ISSU.
- Some FPGA and other firmware updates may not be hitless.

Implementing ISSU

ISSU supports upgrading the System Admin and the XR VM individually. It is mandatory to upgrade the System Admin first and then the XR VM.

System Admin ISSU

- Packages can be System Admin SMUs, Host SMUs, System Admin ISO
- The route processor must have redundancy
- Preparing the installable files before activation is mandatory
- Terminating the process is not supported after the activation starts. Reload the system to restore the old version
- When the image is used to upgrade, the System Admin ISO must be passed along with the host ISO, XR and Sysadmin SMUs
- Commit command will freeze the new version (V2)
- Activation of standby RP is trigerred and then the activation of active RP

XR ISSU

- Packages can be SMUs
- If the image is used, the image must be compatible with the current active image
- The route processor must have redundancy
- Terminating the process is not supported after the activation starts. Reload the system to restore the old version

For upgrade, System Admin ISSU is performed first, followed by XR ISSU. For downgrade, XR ISSU is performed first, followed by System Admin ISSU.

Upgrading SMUs

A Software Maintenance Update (SMU) is a software patch that is installed on the IOS XR device. A SMU is an emergency point fix, which is positioned for expedited delivery and which addresses a network that is down or a problem that affects revenue. A SMU is built on a per release and per component basis and is specific to the platform.

Depending on the process(es) to which the fix is being applied, applying a SMU is non-traffic impacting and the device operation is not compromised.

The two most common SMU upgrades are:

- Process Restart SMU: specific processes are impacted as part of this fix; critical processes remain unimpacted.
- ISSU Reload SMU: specific processes, including critical processes are impacted as part of this fix. The upgrade procedures are discussed in the subesequent pages. OLR-ISSU is implemented for SMUs with SDK changes.

Orchestrated Linecard Reload

Orchestrated Linecard Reload (OLR) is a procedure which enables the user to reload the line cards at different times. This allows a hitless software upgrade for both OTN and packet during ISSU. This overcomes the problem encountered by ISSU wherein, all the line cards are upraded simultaneously and hence causing an outage in cases where there is a SDK change in the software. OLR supports software upgrade involving SDK changes.

Implementing OLR

This section explains the OLR process. Let us consider, upgrading the software from Version-1 to Version-2, where Version-2 has a new SDK.

The working and the protect paths need to be non-overlapping for implementing OLR. The solution requires the network administrator to design the NCS 4000 network with redundant cards in the chassis i.e. each LC is backed up by another LC in the chassis.

For ease of understanding, let us consider, the LCs in the chassis are split into two sets, Red and Green. Each traffic working path needs to have a backup path. The key requirement is that the working and protect paths need to be on LCs that belong to different sets. The first step is to force all traffic on to one set of cards, say, green. This can be done in a controlled manner by setting the admin weights. This can cause a 50ms switchover glitch for certain streams moving to their protect paths in the green set. LCs in the green set are ignored and hence data traffic is not impacted. The LCs in the red set are brought up with Version-2. Once the red set is completely functional, the administrator now switches over the traffic from the green to red set cards by reloading the LCs in the green set. This is the second instance of a 50ms glitch due to the protection switchover. Now all the traffic is on red cards while green cards are upgraded to Version-2. At the end, the administrator can rebalance the traffic streams between the two sets of cards to match the original traffic profile.

Starting from Release 6.5.32, you can upgrade the FPDs of the line cards before performing shutdown and reload of the line cards during OLR workflow. See Performing OLR (Single Chassis System), on page 739.

System Setup (Single Chassis System)

Pre-checks

Perform the following pre-checks:

1. Check for failed configuration using the following command:

```
RP/0/RP0:ios#show configuration failed startup
```

   If there is a configuration failure re-apply the configuration. If the configuration failure persists, use the following command:

```
RP/0/RP0:ios#clear configuration inconsistency

Creating any missing directories in Configuration File system...OK
Initializing Configuration Version Manager...OK
Syncing commit database with running configuration...OK
```

2. All line cards must be installed in plane A or plane B. If any card is not part of the MPLS-TE topology, place it in plane B.

   NCS 4009:

```
RP/0/RP0:ios#show running-config  | in hw-mod
Building configuration...
hw-module olr plane A rack 0 nodes 0,1,2,3,4
hw-module olr plane B rack 0 nodes 5,6,7,8
```

   NCS 4016:

```
RP/0/RP0:ios#show running-config | in hw-module
Building configuration...
hw-module olr plane A rack 0 nodes 0,1,2,3,4,5,6,7
hw-module olr plane B rack 0 nodes 8,9,10,11,12,13,14,15
```

3. Configure the route policy for BGPLU neighbor. To check for BGP-LU neighbors, use the following command:

```
RP/0/RP0:ios#show bgp sessions

Neighbor        VRF                   Spk    AS   InQ  OutQ  NBRState     NSRState
100.1.1.1      default                 0     1     0     0  Established  NSR Ready
53.0.0.2        default                 0     1     0     0  Established  NSR Ready
54.0.0.2        default                 0     1     0     0  Established  NSR Ready
RP/0/RP0:R1#

RP/0/RP0:ios#show running-config route-policy OLR_PLANE_A
route-policy OLR_PLANE_A
if destination in (100.1.1.1/32) then
set weight 6000
else
pass
endif
end-policy
!
RP/0/RP0:ios#show running-config route-policy OLR_PLANE_B
route-policy OLR_PLANE_B
if destination in (100.1.1.1/32) then
set weight 5000
else
pass
endif
```

```
end-policy
!
```

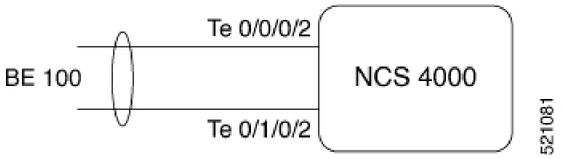
Note We recommend you to set a higher weight for a BGP-LU session.

The running configuration of BGP is shown below:

```
show running-config route-policy OLR_PLANE_A
router bgp 1
neighbor 53.0.0.2
  remote-as 1
  update-source Bundle-Ether2
  address-family ipv4 labeled-unicast
   route-policy PLANE_A in
   route-reflector-client
   next-hop-self
  !
 !
 neighbor 54.0.0.2
  remote-as 1
  update-source Bundle-Ether3
  address-family ipv4 labeled-unicast
   route-policy PLANE_B in
   route-reflector-client
   next-hop-self
  !
```

4. Traffic must be switched from plane A to plane B.

   - **Switch traffic on Active/Active LAG from Plane A to Plane B**



```
int TenGigE 0/0/0/2   >>>>>>>>> Plane A interface
shut
int TenGigE 0/1/0/2  >>>>>>>>>>> Plane B interface
no shut
```

   - To check the traffic from the router, use the following command:

```
RP/0/RP0:ios#show inter TenGigE 0/1/0/1 | in pack
  5 minute input rate 1000 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 0 packets/sec
     31 packets input, 27399 bytes, 0 total input drops
     Received 0 broadcast packets, 26 multicast packets
     29 packets output, 27245 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
```

   - **Switch traffic on BGPLU Plane A to Plane B**

```
route-policy OLR_PLANE_B
  if destination in (100.1.1.1/32) then
    set weight 7000
  else
    pass
  endif
```

```
end-policy
!
```

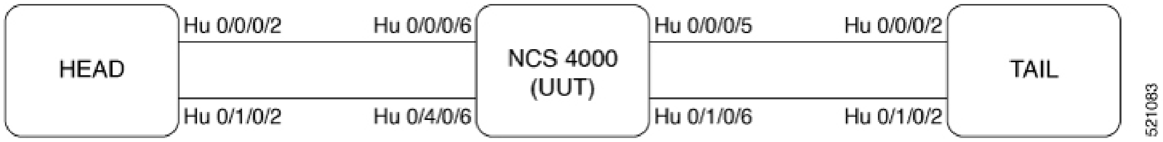
Note A higher weight is recommended.

- **Switch traffic on MPLS enabled Plane A interface to Plane B interface**

```
mpls traffic-eng
 interface HundredGigE0/0/0/5.100
admin-weight 16777200
 !
```

Note 16777200 is the lockout metric used for plane A interfaces.

- **Switch traffic on CORE interfaces**



To check for MPLS-TE interface neighbors, use the following command:

```
RP/0/RP0:ios#show mpls traffic-eng  link-management igp-neighbors
Fri Feb 3 14:13:56.515 IST

  Link ID:: HundredGigE0/0/0/5.100
    Neighbor ID: 0000.0000.000b.03 (IS-IS 100 level 2, link address: 48.0.0.2)
Link ID:: HundredGigE0/0/0/6.100
    Neighbor ID: 0000.0000.000b.03 (IS-IS 100 level 2, link address: 49.0.0.2)
Link ID:: HundredGigE0/4/0/6.100
    Neighbor ID: 0000.0000.000b.03 (IS-IS 100 level 2, link address: 58.0.0.2)
Link ID:: HundredGigE0/1/0/6.100
    Neighbor ID: 0000.0000.000b.03 (IS-IS 100 level 2, link address: 59.0.0.2)
```

To apply plane A admin-weight on the MPLS-TE interfaces:

```
** config on UUT **
mpls traffic-eng
 interface HundredGigE0/0/0/5.100
admin-weight   16777200
 !
 interface HundredGigE0/0/0/6.100
admin-weight   16777200
 !


** config on Peer Nodes **
mpls traffic-eng
 interface HundredGigE0/0/0/2.100
admin-weight   16777200
 !


** config on Peer Nodes **
mpls traffic-eng
```

```
 interface HundredGigE0/0/0/2.100
admin-weight   16777200
 !
```

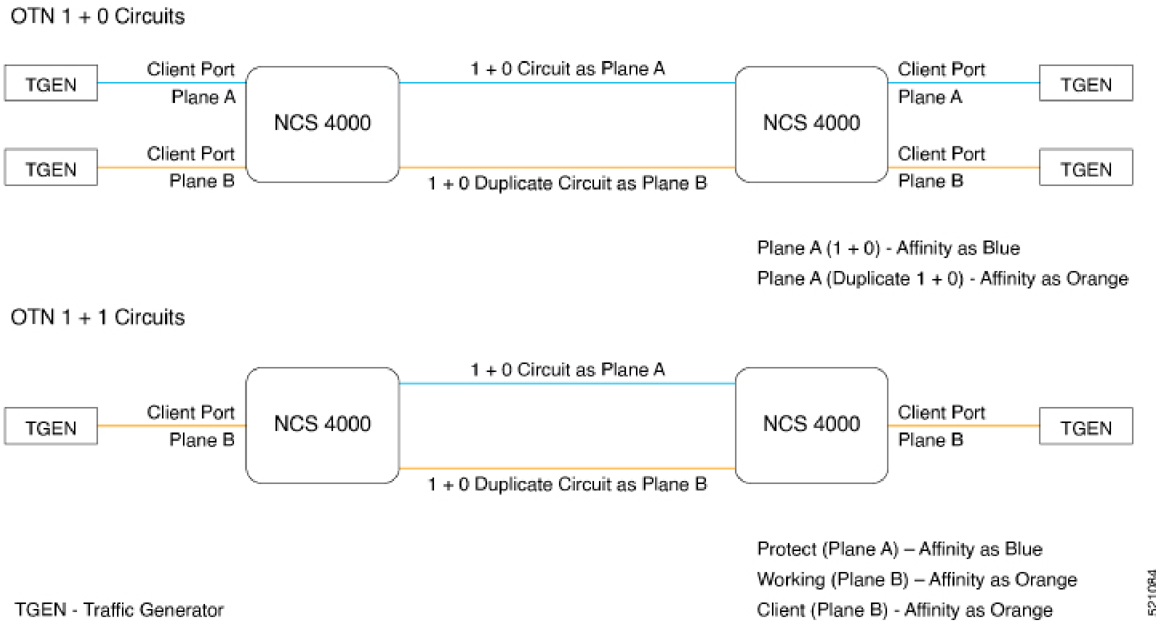
- **Check all the traffic moved to plane B interfaces**

  Verify that both Ingress IF and Egress IF in command output "show mpls traffic-eng forwarding" belongs to the same Plane B.

```
RP/0/RP0:RP1#show mpls traffic-eng forwarding
P2P tunnels:
Tunnel ID                  Ingress IF     Egress IF      In lbl  Out lbl
Backup
-------------------------- -------------- -------------- ------- --------------
-------
49.49.49.49 42149_2227     Hu0/13/0/1.112  Te0/6/0/6/3.1 28597   0
unknown
49.49.49.49 42147_2253     Hu0/13/0/1.112  Te0/6/0/6/3.1 28595   0
unknown
49.49.49.49 42145_2273     Hu0/13/0/1.112  Te0/6/0/6/3.1 28593   0
unknown
49.49.49.49 42150_2283     Hu0/13/0/1.112  Te0/6/0/6/3.1 28598   0
unknown
49.49.49.49 42143_2299     Hu0/13/0/1.112  Te0/6/0/6/3.1 28591   0
unknown
49.49.49.49 42148_2302     Hu0/13/0/1.112  Te0/6/0/6/3.1 28596   0
unknown
```

- **OTN tunnel plane configuration**

  OTN line cards must be part of OLR. For OTN, an additional duplicate circuit must be present in plane B. To configure it, place the active circuit in plane A and the create the duplicate circuit in plane B. The client ports are placed in their respective planes.



Sample Configuration

```
mpls traffic-eng
   controller Odu-Group-Te 0
   logging events lsp-status state
   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 ODU3
   static-uni ingress-port controller OTU30/8/0/5 egress-port unnumbered 55
   destination ipv4 unicast 10.106.201.222
  path-option 1 dynamic attribute-set otn_olr_planeB_W_orange protected-by 2 lockdown

   path-option 2 dynamic attribute-set otn_olr_planeA_P_brown lockdown
  !
 attribute-set path-option otn_olr_planeA_R_blue
  affinity include blue
 !
 attribute-set path-option otn_olr_planeA_P_brown
  affinity include brown
 !
 attribute-set path-option otn_olr_planeB_W_orange
  affinity include orange
```

Note The affinities used in the sample configuration are generic and used only for traffic switching.

Verification

```
RP/0/RP0:ios#show controllers Odu-Group-Te0 protection-detail
ODU  Group Information
--------------------------------------------------------------
LOCAL
                Request State                  : Do Not Revert State
                Request signal                 : 1
                Bridge signal                    : 1
                Bridge Status                   : 1+1
REMOTE
                Request State                 : Do Not Revert State
                Request signal                : 1
                Bridge signal                   : 1
                Bridge Status                  : 1+1
WORKING
                Controller Name            : ODU31_1_0_0_43
                ODU STATE                        : Active_tx
                Local Failure                       : State Ok
                Remote Failure                  : Not Applicable
                WTR Left                             : 0 ms
PROTECT
                Controller Name                : ODU30_8_0_1_83
                ODU STATE                        : Active
                Local Failure                       : State Ok
                Remote Failure                  : Not Applicable
                WTR Left                             : 0 ms
```

Note The ODU-Te 0 has both an active and protect path.

Note The *reoptimize timers delay installation* parameter is set to 180 seconds. Hence, wait for 180 Seconds after applying the lockout metric on Plane A interfaces.

- **Apply the Max metric on Plane B interfaces**

```
** config on UUT **
mpls traffic-eng
 interface HundredGigE0/4/0/6.100
admin-weight   4294967295
 !
 interface HundredGigE0/1/0/6.100
admin-weight   4294967295
 !


** config on Peer Node**
mpls traffic-eng
 interface HundredGigE0/1/0/2.100
admin-weight   4294967295
 !


** config on Peer Node **
mpls traffic-eng
 interface HundredGigE0/1/0/2.100
admin-weight   4294967295
 !
```

Note 4294967295 is the max metric used for plane B interfaces.

- Add the V2 image to the router from the sftp path.

```
RP/0/RP0:ios: install add source
sftp://test@10.127.60.201://nobackup/tftpboot/images/MC_DT/6533_I/
ncs4k-mpls.pkg-6.5.33 ncs4k-mgbl.pkg-6.5.33 ncs4k-k9sec.pkg-6.5.33
ncs4k-mini-x-6.5.33.iso <SMUs>
```

After it is done, check the admin repository to verify.

```
RP/0/RP1:ios#show install repository all
2 package(s) in Host repository:
    host-6.5.33
    host-6.5.32
4 package(s) in Admin repository:
    ncs4k-mini-x-6.5.33
    ncs4k-sysadmin-6.5.33
    ncs4k-mini-x-6.5.32
    ncs4k-sysadmin-6.5.32
17 package(s) in XR repository:
    ncs4k-mini-x-6.5.33
    ncs4k-mgbl-6.5.33
    ncs4k-k9sec-6.5.33
    ncs4k-6.5.32.CSCwe17425-0.0.3.i
    ncs4k-mpls-6.5.33
    ncs4k-mpls-6.5.32
    ncs4k-6.5.33.CSCvz67358-0.0.7.i
    ncs4k-xr-6.5.32
    ncs4k-6.5.32.CSCwd69083-0.0.13.i
```

```
ncs4k-mgbl-6.5.32
ncs4k-6.5.32.CSCvz67358-0.0.6.i
ncs4k-xr-6.5.33
ncs4k-k9sec-6.5.32
ncs4k-mini-x-6.5.32
ncs4k-6.5.33.CSCwe11655-0.0.8.i
ncs4k-6.5.32.CSCwc68365-0.0.6.i
ncs4k-6.5.33.CSCwe17425-0.0.5.i
```

5. Verify the cross plane traffic. See the *OLR MOP document, Release 6.5.33* for more information.

Install System Admin Package Using ISSU (Single Chassis System)

This task enables the user to upgrade the System Admin package. While performing ISSU, the System Admin package is upgraded first, followed by the XR packages. The System Admin upgrade must be performed node by node.

Procedure

Step 1 Use the **show install repository all** to display the *mini* package and the other packages of the new software version.

Example:

```
 sysadmin-vm:0_RP1# show install repository all
Fri Feb  3  07:34:43.264 UTC+00:00
 Admin repository
---------------------
 ncs4k-mini-x-6.5.33
 ncs4k-sysadmin-6.5.33
 ncs4k-mini-x-6.5.32
 ncs4k-sysadmin-6.5.32
  XR repository
------------------
 ncs4k-mini-x-6.5.33
  ncs4k-mgbl-6.5.33
  ncs4k-k9sec-6.5.33
  ncs4k-6.5.32.CSCwe17425-0.0.3.i
   ncs4k-mpls-6.5.33
   ncs4k-mpls-6.5.32
   ncs4k-6.5.33.CSCvz67358-0.0.7.i
   ncs4k-xr-6.5.32
   ncs4k-6.5.32.CSCwd69083-0.0.13.i
   ncs4k-mgbl-6.5.32
   ncs4k-6.5.32.CSCvz67358-0.0.6.i
   ncs4k-xr-6.5.33
   ncs4k-k9sec-6.5.32
   ncs4k-mini-x-6.5.32
   ncs4k-6.5.33.CSCwe11655-0.0.8.i
   ncs4k-6.5.32.CSCwc68365-0.0.6.i
   ncs4k-6.5.33.CSCwe17425-0.0.5.i



  Host repository
```

```
--------------------
host-6.5.33
host-6.5.32
sysadmin-vm:0_RP1#
```

Step 2 Run the command **install extract** *mini_package* from System Admin VM to extract the host and ISO file for System Admin installation.

Example:

```
sysadmin-vm:0_RP1#  install extract ncs4k-mini-x-<release-version>
```

Step 3 Prepare the installable files before activation using the command **install prepare** *ncs4k-sysadmin-<release-version>host-<release-version>sysadminSMU<release-version>*

Example:

```
sysadmin-vm:0_RP1# install prepare ncs4k-sysadmin-<release-version> host-<release-version>
Package list:
result Fri Feb 03 07:50:50 2023 Install operation 73 (install prepare) started by user
'root' will continue asynchronously.
sysadmin-vm:0_RP1#
```

Step 4 Check the current status of the RP1 and RP0 using the command **show redundancy summary**

Example:

```
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)
```

Step 5 Use the **install activate nodes 0/standbyRP** to enable the package configurations to be made active on the router so new features and software fixes take effect.

Standby RP reloads and comes up with version2 host and sysadmin. Redundancy is established and NSR is also ready.

a) Log in to Active RP System Admin console.

Example:

```
telnet 10.106.201.XX 20XX
Trying 10.106.201.13...
Connected to 10.106.201.XX.
Escape character is '^]'.
System Admin Username: root
Password:
root connected from 127.0.0.1 using console on sysadmin-vm:0_RP0
sysadmin-vm:0_RP0#
```

b) Activate the node to the new version using the command **install activate** *Standby RP*

```
sysadmin-vm:0_RP0# install activate nodes 0/RP1
This install operation will result in system reload
Do you want to proceed [yes/no]: yes
Proceeding with operation
result Fri Feb 03 07:13:35 2023 Install operation 74 (install activate) started by user
 'root' will continue asynchronously.
sysadmin-vm:0_RP0#
Fri Feb 03 07:15:36 2023 Install operation 74 completed successfully.
```

The nodes must be upgraded one by one. Ensure that redundancy is established.

Note Before upgrading the Active RP System Admin, execute the **mpls traffic-eng reoptimize all** command and wait for 10 mins, because the reoptimize timers delay installation and reoptimize timers delay cleanup are set to 180 seconds in the router. This makes sure to avoid any reoptimization being triggered during ISSU upgrade and system can take 10 minutes to handle the manual reoptimization.

Step 6 Activate the node.

Active RP reloads and comes up with version2 host and sysadmin. Redundancy is established as both RPs are on now same images.

a) Log in to System Admin active RP console.

```
telnet 10.106.201.XX 20XX
Trying 10.106.201.13...
Connected to 10.106.201.XX.
Escape character is '^]'.
System Admin Username: root
Password:
root connected from 127.0.0.1 using console on sysadmin-vm:0_RP0
sysadmin-vm:0_RP0#
```

b) Activate the node to the new version using the command **install activate nodes** *Active RP*

```
sysadmin-vm:0_RP0# install activate nodes 0/RP0
Do you want to proceed [yes/no]: yes
Proceeding with operation

result Fri Feb 03 08:49:28 2023 Install operation 75 (install activate) started by user
 'root' will continue asynchronously.
Fri Feb 03 08:49:49 2023 Install operation 75 completed successfully.
Fri Feb 03 08:51:28 2023 Card will now reload as part of the install operation.
```

Step 7 Commit the new System Admin and host images.

a) Log in to System Admin RP console:

Example:

```
telnet 10.106.201.XX 20XX
Trying 10.106.201.13...
Connected to 10.106.201.XX.
Escape character is '^]'.
System Admin Username: root
Password:
root connected from 127.0.0.1 using console on sysadmin-vm:0_RP0
sysadmin-vm:0_RP0#
```

b) Commit the newly activated software using the command **install commit**.

Example:

```
sysadmin-vm:0_RP1# show install active
Fri Feb  3  09:03:56.187 UTC+00:00
 Node 0/RP0 [RP]
    Active Packages: 1
       ncs4k-sysadmin-6.5.33 version=6.5.33 [Boot image]


 Node 0/RP1 [RP]
    Active Packages: 1
       ncs4k-sysadmin-6.5.33 version=6.5.33 [Boot image]


sysadmin-vm:0_RP1# install commit
```

```
result Fri Feb 03 10:28:23 2023 Install operation 76 (install commit) started by user
'root' will continue asynchronously.
sysadmin-vm:0_RP1# Fri Feb 03 10:30:23 2023 Install operation 76 completed successfully.
```

Step 8 Verify the activated software using the command **show install committed**.

Example:

```
sysadmin-vm:0_RP1# show install committed
Fri Feb  3  09:03:57.187 UTC+00:00
 Node 0/RP0 [RP]
    Active Packages: 1
       ncs4k-sysadmin-6.5.33 version=6.5.33 [Boot image]

 Node 0/RP1 [RP]
    Active Packages: 1
       ncs4k-sysadmin-6.5.33 version=6.5.33 [Boot image]
```

Install XR Packages Using ISSU

Complete this task to upgrade the system or install a patch. The system upgrade is done using an ISO image file, while the patch installation is done using packages and SMUs.

Before you begin

- Verify the status of route processor redundancy.

```
RP/0/RP0:R1#show redundancy summary
    Active Node    Standby Node
    -----------    ------------
          0/RP0        0/RP1 (Node Ready, NSR:Ready)
          0/LC0        0/LC1 (Node Ready, NSR:Not Configured)

RP/0/RP0:R1#
```

- Verify Cross plane traffic. See *OLR MOP document, Release 6.5.33*.
- Make sure that the V2 image is present in the repository.

Procedure

Step 1 To extract the XR image from ncs4k-x.iso and place it in the repository use the command **install extract** *package_name*.

Example:

```
P/0/RP1:router#install extract ncs4k-mini-x-release-version
```

Step 2 Verify that the XR image files are properly extracted to repository using the command **show install repository all**.

Example:

```
P/0/RP1:router#show install repository all
2 package(s) in Host repository:
    host-6.5.33
    host-6.5.32
4 package(s) in Admin repository:
    ncs4k-mini-x-6.5.33
    ncs4k-sysadmin-6.5.33
    ncs4k-mini-x-6.5.32
    ncs4k-sysadmin-6.5.32
17 package(s) in XR repository:
    ncs4k-mini-x-6.5.33
    ncs4k-mgbl-6.5.33
    ncs4k-k9sec-6.5.33
    ncs4k-6.5.32.CSCwe17425
    ncs4k-mpls-6.5.33
    ncs4k-mpls-6.5.32
    ncs4k-6.5.33.CSCvz67358-0.0.7.i
    ncs4k-xr-6.5.32
    ncs4k-6.5.32.CSCwd69083-0.0.13.i
    ncs4k-mgbl-6.5.32
    ncs4k-6.5.32.CSCvz67358-0.0.6.i
    ncs4k-xr-6.5.33
    ncs4k-k9sec-6.5.32
    ncs4k-mini-x-6.5.32
    ncs4k-6.5.33.CSCwe11655-0.0.8.i
    ncs4k-6.5.32.CSCwc68365-0.0.6.i
    ncs4k-6.5.33.CSCwe17425-0.0.5.i

RP/0/RP1:Router#
```

Step 3 Activate the upgrade to the new version using the command **install activate issu** *package_name*.

Example:

```
: router # install activate issu ncs4k-mpls-6.5.33 ncs4k-xr-6.5.33
 ncs4k-mgbl-6.5.33 ncs4k-k9sec-6.5.33
Feb 03 14:26:52 Package list:
Feb 03 14:26:52     ncs4k-mgbl-6.5.33
Feb 03 14:26:52     ncs4k-k9sec-6.5.33
Feb 03 14:26:52     ncs4k-mpls-6.5.33
Feb 03 14:26:52     ncs4k-6.5.33.CSCvz67358-0.0.7.i
Feb 03 14:26:52     ncs4k-xr-6.5.33
Feb 03 14:26:52     ncs4k-6.5.33.CSCwe11655-0.0.8.i
Feb 03 14:26:52     ncs4k-6.5.33.CSCwe17425-0.0.5.i
Feb 03 14:26:53 Action 1: install prepare action started
Feb 03 14:26:53 Install operation will continue in the background
Feb 03 14:27:38 The prepared software is set to be activated with ISSU
Feb 03 14:28:03 Checking compatibility with sysadmin
Feb 03 14:28:03 This install operation will start the issu, continue?
 [yes/no]:[yes] yes
```

Step 4 Commit the newly activated software using the command **install commit**.

Example:

```
RP/0/RP0:R1##install commit
Feb 03 15:28:30 Install operation 67 started by root:
  install commit
Feb 03 15:28:31 Install operation will continue in the background
RP/3/RP1:R1#Feb 03 15:28:53 Install operation 67 finished successfully

RP/3/RP1:R1#
```

Commits the package.

Performing OLR (Single Chassis System)

Procedure

Step 1 Use the command **show controllers fia driver location all | in fia** to displays the status of the NPU on all the cards.

Example:

```
RP/0/RP1:R1##show controllers fia driver location all  | in fia
Asics :
HP - HotPlug event, PON - Power On reset
HR - Hard Reset,    WB  - Warm Boot
+----------------------------------------------------------------------------------+
| Asic inst. | fap|HP|Slice|Asic|Admin|Oper | Asic state |   Last   |PON|HR |MODE  |
|  (R/S/A)   | id |  |state|type|state|state|            |   init   |(#)|(#)|STATE |
+----------------------------------------------------------------------------------+
| 0/0/0      |   0| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
| 0/2/0      |   2| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
| 0/8/0      |   4| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
| 0/1/0      |   6| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
| 0/4/0      |   8| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
| 0/11/0     |  10| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
```

The line cards listed under plane A and plane B will be indicated as SDKLESS.

Step 2 Perform FPD upgrade for plane A line cards:

Use this step when FPD upgrade is required. For upgrade from 6.5.32 to 6.5.33, FPD upgrade is not required.

a) Verify LC distribution between plane A and plane B

```
:
RP/0/RP0:R1#show running-config  | in hw-mod
Building configuration...
hw-module olr plane A rack 0 nodes 0,2,8
hw-module olr plane B rack 0 nodes 1,4,11
```

b) Check the FPDs for the line cards:

```
RP/0/RP0:R1#show hw-module fpd | e CURRENT
                                                               FPD Versions
                                                              =================Location
   Card type        HWver FPD device       ATR Status   Running Programd
------------------------------------------------------------------------------
0/0       NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/0       NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/2       NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/2       NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/8       NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/8       NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/1       NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/1       NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/4       NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/4       NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
```

```
0/11      NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/11      NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/RP0     NCS4K-RP          0.1   Timing-FPGA       S  NEED UPGD  4.42    4.42
0/RP1     NCS4K-RP          0.1   Timing-FPGA       S  NEED UPGD  4.42    4.42
```

Note During OLR, FPD upgrade is done only on the line cards. And, only one card upgrade is done at a time.

c) Upgrade the FPD of plane A line cards using one of the following commands:

Command to upgrade the FPDs:

```
upgrade hw-module location <slot > fpd all
 upgrade hw-module location <slot > fpd <fpd name>
```

Step 3 Shut down the plane A cards using the **hw-module location** *location-id* **shutdown** command.

Example:

```
RP/0/RP0:ios#admin

root connected from 127.0.0.1 using console on xr-vm
sysadmin-vm:0_RP1# hw-module location 0/0 shutdown
Shutdown hardware module ? [no,yes] yes
result Card graceful shutdown request on 0/0 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/2 shutdown
Shutdown hardware module ? [no,yes] yes
result Card graceful shutdown request on 0/2 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/8 shutdown
Shutdown hardware module ? [no,yes] yes
result Card graceful shutdown request on 0/8 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **
```

Step 4 Reload the plane A cards using the **hw-module location** *location-id* **reload** command.

Example:

```

sysadmin-vm:0_RP1# hw-module location 0/0 reload
Reload hardware module ? [no,yes] yes
result Card graceful reload request on 0/0 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/2reload
Reload hardware module ? [no,yes] yes
result Card graceful reload request on 0/2 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/8 reload
Reload hardware module ? [no,yes] yes
result Card graceful reload request on 0/8 succeeded.
```

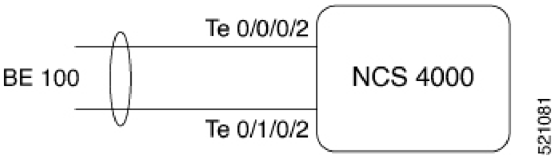
```
sysadmin-vm:0_RP1#

** wait for 30 seconds **
```

Note Shutting down and reloading the cards is done one by one. We recommend to have a time interval of one minute before shutting down and reloading the next card.

Before proceeding to the next step, wait till all the interfaces and L3 protocols come up.

```
RP/0/RP1:R1##show controllers fia driver location all  | in fia
<< snip >>

Asics :
HP - HotPlug event, PON - Power On reset
HR - Hard Reset,    WB  - Warm Boot
+----------------------------------------------------------------------------------+
| Asic inst. | fap|HP|Slice|Asic|Admin|Oper | Asic state |   Last   |PON|HR |MODE  |
|  (R/S/A)   | id |  |state|type|state|state|            |   init   |(#)|(#)|STATE |
+----------------------------------------------------------------------------------+
| 0/0/0      |   0| 1| NA  | fia| UP  | UP  |ONLINE      |PON  |  1|  0|Fabric|
| 0/2/0      |   2| 1| NA  | fia| UP  | UP  |ONLINE      |PON   |  1|  0|Fabric|
| 0/8/0      |   4| 1| NA  | fia| UP  | UP  |ONLINE      |PON   |  1|  0|Fabric|
| 0/1/0      |   6| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
| 0/4/0      |   8| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
| 0/11/0     |  10| 1| NA  | fia| UP  | NA  |ONLINE      |Sdkless   |  0|  0|Fabric|
```

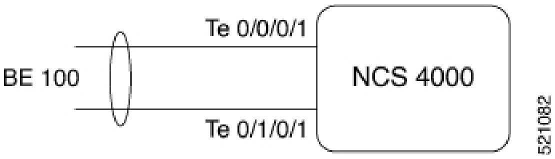
Step 5 Switch traffic on the active-active LAG interface from plane B to plane A.



Example:

```
int TenGigE 0/0/0/2
no shut
int TenGigE 0/1/0/2
shut
```

Step 6 Switch traffic on the active-standby LAG interface from plane B to plane A.



Example:

```
int TenGigE 0/0/0/1
bundle port-priority 33000
int TenGigE 0/1/0/1
bundle port-priority 34000
```

Step 7 Switch traffic on the BGPLU Plane B to Plane A

Example:

```
route-policy OLR_PLANE_B
  if destination in (100.1.1.1/32) then
    set weight 5000
  else
```

```
    pass
  endif
end-policy
!
```

Step 8 Switch traffic from plane B to plane A (bundle).

a. In the case of VPWS LAG or BGP LU and MPLS-TE, perform these steps:

- Remove the lockout metric on plane A core interface (TE) and then apply lockout on plane B interfaces. Wait for 180 seconds. Wait for the TE to switch from plane B to plane A.
- Switch AC LAG or BGP LU from plane B to plane A.

b. In case of VPWS LAG and FLEX (revertive), remove lockout metric on plane A and switch AC LAG from plane B to plane A.

c. In case of VPWS LAG and FLEX (nonrevertive), remove lockout on plane A, apply lockout on plane B, and switch AC LAG from plane B to plane A.

Step 9 Switch traffic from plane B to A. Remove plane A lockout metric and apply lockout metric on plane B interface.

Example:

```
** config on UUT **
mpls traffic-eng
 interface HundredGigE0/0/0/5.100
admin-weight   1000
 !
 interface HundredGigE0/0/0/6.100
admin-weight   1000
 !


** config on Peer Nodes **
mpls traffic-eng
 interface HundredGigE0/0/0/2.100
admin-weight   1000
 !


** config on Peer Nodes **
mpls traffic-eng
 interface HundredGigE0/0/0/2.100
admin-weight   1000
 !
```

For the flex-LSP , wait till the backup path (plane A interface) comes up. Then apply the lockout metric on plane B interfaces.

```
sh mpls lsd  forwarding  tunnels  151
Tunnel_Intf, Path_Info: <Type>
tunnel-te151, (TE-Control), local_lbl=24138, 1 Paths,
        Owner=TE-Control(A)
   1/1: TEv4, 'default':4U, Hu0/4/0/6.100, nh=202.202.202.1, lbl=24030, tun=tt151, weight=0x0,
 class=0x0 bkup=Hu0/0/0/5.100 mrg_lbl=3, bkup_local_lbl=24432, bkup_nh=102.102.102.1,
nnh=0.0.0.0
            flags=0x200 ()
```

In the output displayed above, the bkup=Hu0/0/0/5.10 (Plane A interface) has come up. Apply the lockout metric to plane B.

```
** config on UUT **
mpls traffic-eng
 interface HundredGigE0/4/0/6.100
admin-weight   16777200
 !
 interface HundredGigE0/1/0/6.100
admin-weight   16777200
 !


** config on Peer Nodes **
mpls traffic-eng
 interface HundredGigE0/1/0/2.100
admin-weight   16777200
 !


** config on Peer Nodes **
mpls traffic-eng
 interface HundredGigE0/1/0/2.100
admin-weight   16777200
```

Step 10 Perform FPD upgrade for plane B line cards:

a) Verify LC distribution between plane A and plane B

```
:   RP/0/RP0:R1#sh running-config  | in hw-mod
Building configuration...
hw-module olr plane A rack 0 nodes 0,2,8
hw-module olr plane B rack 0 nodes 1,4,11
```

b) Check the FPDs for the line cards:

```
RP/3/RP1:R1#sh hw-module fpd | e CURRENT
                                                              FPD Versions
                                                            =================Location
   Card type        HWver FPD device       ATR Status   Running Programd
----------------------------------------------------------------------------
0/1       NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/1       NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/4       NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/4       NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/11      NCS4K-4H-OPW-QC2  0.1   CCC-FPGA             NEED UPGD  1.01    1.01
0/11      NCS4K-4H-OPW-QC2  0.1   Primary-ZYNQ      S  NEED UPGD  4.11    4.11
0/RP0     NCS4K-RP          0.1   Timing-FPGA       S  NEED UPGD  4.42    4.42
0/RP1     NCS4K-RP          0.1   Timing-FPGA       S  NEED UPGD  4.42    4.42
```

Note During OLR, FPD upgrade is done only on the line cards. And, only one card upgrade is done at a time.

c) Upgrade the FPD of plane B line cards using one of the following commands:

Command to upgrade the FPDs:

```
upgrade hw-module location <slot > fpd all
 upgrade hw-module location <slot > fpd <fpd name>
```

Step 11 Shut and reload all the line cards of the plane B interface.

Example:

```
RP/0/RP0:ios#admin

root connected from 127.0.0.1 using console on xr-vm
sysadmin-vm:0_RP1# hw-module location 0/1 shutdown
```

```
Shutdown hardware module ? [no,yes] yes
result Card graceful shutdown request on 0/1 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/4 shutdown
Shutdown hardware module ? [no,yes] yes
result Card graceful shutdown request on 0/4 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/11  shutdown
Shutdown hardware module ? [no,yes] yes
result Card graceful shutdown request on 0/11 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/1 reload
Reload hardware module ? [no,yes] yes
result Card graceful reload request on 0/1 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/4 reload
Reload hardware module ? [no,yes] yes
result Card graceful reload request on 0/4 succeeded.
sysadmin-vm:0_RP1#

** wait for 30 seconds **

sysadmin-vm:0_RP1# hw-module location 0/11 reload
Reload hardware module ? [no,yes] yes
result Card graceful reload request on 0/11succeeded.
sysadmin-vm:0_RP1#

  ** wait for 30 seconds **

RP/0/RP1:R1##show controllers fia driver location all  | in fia
<< snip >>

Asics :
HP - HotPlug event, PON - Power On reset
HR - Hard Reset,    WB  - Warm Boot
+----------------------------------------------------------------------------------+
| Asic inst. | fap|HP|Slice|Asic|Admin|Oper | Asic state |   Last   |PON|HR |MODE  |
|  (R/S/A)   | id |  |state|type|state|state|            |   init   |(#)|(#)|STATE |
+----------------------------------------------------------------------------------+
| 0/0/0      |   0| 1| NA  | fia| UP  | UP  |ONLINE      |PON  |  1|  0|Fabric|
| 0/2/0      |   2| 1| NA  | fia| UP  | UP  |ONLINE      |PON   |  1|  0|Fabric|
| 0/8/0      |   4| 1| NA  | fia| UP  | UP  |ONLINE      |PON   |  1|  0|Fabric|
| 0/1/0      |   6| 1| NA  | fia| UP  | UP  |ONLINE      |PON   |  1|  0|Fabric|
| 0/4/0      |   8| 1| NA  | fia| UP  | UP  |ONLINE      |PON   |  1|  0|Fabric|
| 0/11/0     |  10| 1| NA  | fia| UP  | UP  |ONLINE      |PON   |  1|  0|Fabric|
-----------------------------------------------------------------------------------------
```

Ensure all the line cards of the plane A and B interfaces are in PON state.

Step 12 Remove the plane B lockout metric.

Example:

```
** config on UUT **
mpls traffic-eng
 interface HundredGigE0/4/0/6.100
admin-weight   1000
 !
 interface HundredGigE0/1/0/6.100
admin-weight   1000
 !


** config on Peer nodes**
mpls traffic-eng
 interface HundredGigE0/1/0/2.100
admin-weight   1000
 !


** config on Peer nodes **
mpls traffic-eng
 interface HundredGigE0/1/0/2.100
admin-weight   1000
 !
```

Step 13 Remove the route policy for the BGP LU neighbor.

Example:

```
Conf t
no route-policy OLR_PLANE_A
       no route-policy OLR_PLANE_B
       commit
router bgp 1
 neighbor 101.6.1.2
  address-family ipv4 labeled-unicast
  no  route-policy OLR_PLANE_B in
 neighbor 101.6.1.6
  address-family ipv4 labeled-unicast
   no route-policy OLR_PLANE_A in
commit
end
```

Step 14 Verify that all services and up. ISSU and OLR processes are complete.

Note

- Y1564 test is not supported, when the line cards are in sdkless state.
- Connectivity Fault Management (CFM) peer Maintenance End Points (MEPs) are in timed out state when the line cards are in sdkless state.

Step 15 Verify and upgrade the FPDs.

Use this step when FPD upgrade is required. For upgrade from 6.5.32 to 6.5.33, FPD upgrade is not required.

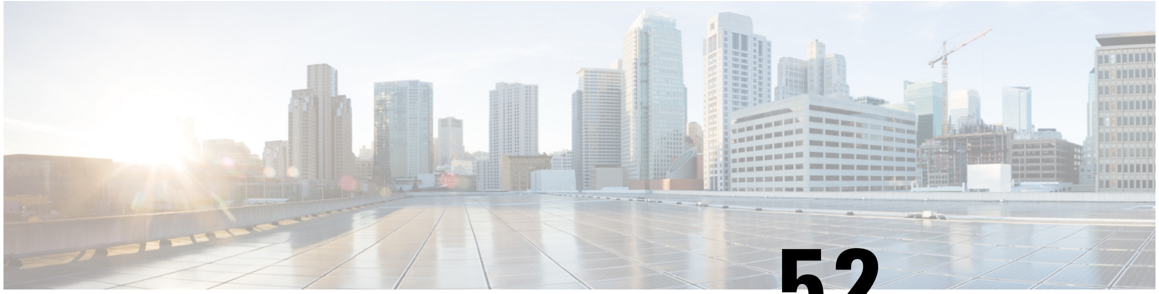
Example:

```
RP/0/RP0:R1#show hw-module fpd | e CURRENT
                                                               FPD Versions
                                                           ==================
 Location   Card Type                     HWver FPD device    ATR Status    Running Programd
------------------------------------------------------------------------------
0/RP0     NCS4K-RP          0.1             Timing-FPGA       S  NEED UPGD  4.42    4.42
0/RP1     NCS4K-RP          0.1             Timing-FPGA       S  NEED UPGD  4.42    4.42
```

To upgrade the FPDs, use the command, **upgrade hw-module location** *slot* **fpd all.**

Note Only one card upgrade is done at a time.

While upgrading the FPDs, upgrade the line cards first, followed by the fabric cards, and finally the RP cards. After each upgrade, reload the card.



CHAPTER 52

Capture Logs

This chapter describes the Cisco IOS XR commands to trace logs for configuration manager, OTN controllers, ptah, system database and pfi.

Capture System Database Logs

Before you begin

Procedure

show tech-support sysdb

Example:

```
RP/0/RP0:hostname #show tech-support sysdb
```

This generates a zip file containing trace logs of debugging issues of system database.

Capture ptah Logs

Before you begin

Procedure

show tech-support ptah

Example:

```
RP/0/RP0:hostname # show tech-support ptah
```

This generates a zip file containing trace logs of debugging transport alarm library.

Capture Ifmanager Logs

Procedure

show tech-support pfi

Example:

```
RP/0/RP0:hostname #show tech-support pfi
```

This generates a zip file containing trace logs of debugging ifmanager issues.

Capture OTN Logs

Before you begin

Procedure

show tech-support otn

Example:

```
RP/0/RP0:hostname #show tech-support otn
```

This generates a zip file containing trace logs of debugging OTN controllers .

Capture Configuration Manager Logs

Before you begin

Procedure

show tech-support cfgmgr

Example:

```
RP/0/RP0:hostname #show tech-support cfgmgr
```

This generates a zip file containing trace logs of debugging issues of configuration (any controller).

CHAPTER 53

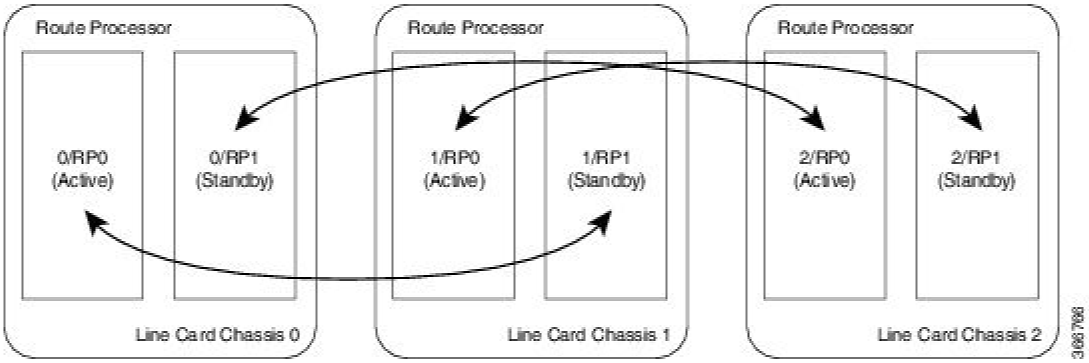
Inter-Rack RP Pairing

This chapter provides details regarding inter-rack RP pairing in the Cisco NCS 4000 Series Router.

Inter-rack RP Pairing

In a multi chassis (MC) system, the active-standby RP pairing in a single rack is called intra-rack pairing. There is a possibility that the rack which houses the active VM and standby VM may go down. This results in the reboot of all the line card chassis, thus impacting traffic of the MC system. Inter-rack (or cross-rack) pairing allows pairing route processors (RP) between racks to provide high availability (HA) against rack failures. The RP of one rack is paired with the RP on the next rack. The pairing is determined by the SDR manager through a daisy chain algorithm. The algorithm is executed only on the discovered set of nodes. The pairing remains consistent as long as the set of nodes that were discovered is constant.

Figure 40: Example for inter-rack pairing



Only the racks with dual RPs (an RP on both slots of the rack) are considered for inter-rack pairing. The pairing algorithm is triggered automatically when:

- a rack is inserted
- a change in chassis configuration is committed
- RP is re-inserted (or replaced)
- re-pair command is manually executed
- change in configuration between inter-rack and intra-rack pairing, and vice-versa

Inter-rack pairing is triggered manually or automatically, when:

- an RP is added or deleted
- an OIR is performed for an RP

System Readiness

The system must be ready before and after enabling inter-rack pairing. Run these commands to improve debuggability and compare their output to expected behavior. This ensures that the system is ready, and any changes in System Admin are reflected in XR VMs.

Table 53: Commands used to check the system readiness

Description	Commands
Verify all the nodes are in Operational state and a Standby RP is available in Ready state	**SysAdmin VM:** • show sdr default-sdr pairing • show platform • show platform slice • show vm • show vm • show version • show inventory • show log • show install log • show run • dir:harddisk **XR-VM:** • show redundancy • show platform vm • show placement program all • show health gsp • show health sysdb • show platform • show log • show run • cfs check • dir harddisk:

Description	Commands
Verify the fabric health and system environment. Ensure all fabric planes are Up and fan speed is not zero.	**SysAdmin VM:** • show controller fabric health • show controller fabric plane all • show alarms detail • show environment power • show environment fan • show environment temp

Enable Inter-rack Pairing Mode

The default mode is intra-rack. The pairing algorithm is run when inter-rack (cross-rack) pairing mode is enabled for a multi chassis system. Traffic loss may occur when moving between inter-rack and intra-rack pairing modes. All cross-rack related triggers must be done in a maintenance window.

Procedure

Step 1 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters sysadmin configuration mode.

Step 2 **sdr defautlt-sdr pairing-mode inter-rack**

Example:

```
sysadmin-vm:0_RP0(config) # sdr default-sdr pairing-mode
inter-rack
```

Enable inter-rack pairing mode.

Step 3 **commit**

Example:

```
sysadmin-vm:0_RP0(config) # commit
```

Commits the configuration changes.

Step 4 **show sdr default-sdr pairing**

Example:

```
sysadmin-vm:0_RP0 # show sdr default-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
```

Displays the pairing details.Verify that the pairing is inter-rack and the partner nodes are on different racks.

Initiate Re-pair

The user can manually initiate re-calculation of the inter-rack pairing algorithm. This task changes the pairing based on the current state of the card inventory.

Procedure

Step 1 **sdr default-sdr re_pair**

Example:

```
sysadmin-vm:0_RP1# sdr default-sdr re_pair
```

Displays the current configuration and the prediction for the re_paired configuration. If any rack is down, the sdr default-sdr re_pair command optimizes the pairing based on this change.

Step 2 **show sdr default-sdr pairing**

Example:

```
sysadmin-vm:0_RP0#show sdr default-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
```

Displays the updated inter-rack pairing information.

Usecases for re-pairing RPs

This section describes the scenarios where manual or automatic re-pairing of RPs is required.

Automatic re-pairing is initiated when:

- a rack is inserted
- a rack is removed
- an RP is inserted to create dual RP

Manually re-pairing is initiated when:

- a rack failure is detected
- an RP is reinserted (as part of OIR of an RP)
- RP is removed from SDR

Re-pair due to Rack Insertion

This task shows the automatic recalculation of the pairing algorithm when a rack is inserted.

Use the following commands to check the current status of the chassis:

- **show chassis**
- **show redundancy**
- **show sdr default-sdr pairing**
- **show running-config chassis**

Procedure

Step 1 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters sysadmin configuration mode.

Step 2 **chassis serial** *serial number* **rack** *rack-id*

Example:

```
sysadmin-vm:F1_SC0(config)# chassis serial FLM171762WW rack 1
```

Enters the chassis cofiguration mode. Associates a rack number to the chassis.

Step 3 **commit**

Commits the configuration changes.

Step 4 Insert a rack.

Step 5 **show chassis**

Example:

```
Serial Num    Rack Num    Rack Type   Rack State  Data Plane  Ctrl Plane
--------------------------------------------------------------------------
FLM213101U5   F1          FCC         OPERATIONAL CONN        CONN
FLM213200BF   F0          FCC         OPERATIONAL CONN        CONN
FLM213200BR   F3          FCC         OPERATIONAL CONN        CONN
FLM21330065   F2          FCC         OPERATIONAL CONN        CONN
SAL1834ZBRN   1           LCC         OPERATIONAL CONN        CONN
SAL2016PB3Z   3           LCC         OPERATIONAL CONN        CONN
SAL205100M2   0           LCC         OPERATIONAL CONN        CONN
SAL2106055V   2           LCC         OPERATIONAL CONN        CONN
```

Verify if the newly inserted rack is visible.

Step 6 **show running-config chassis**

Example:

```
show running-config chassis Wed Jan  23 14:57:02.618 UTC-05:30 chassis serial FLM213101U5
 rack F1 !
chassis serial FLM213200BF
 rack F0
!
chassis serial FLM213200BR
 rack F3
!
chassis serial FLM21330065
 rack F2
!
chassis serial SAL1834ZBRN
 rack 1
!
chassis serial SAL2016PB3Z
 rack 3
!
chassis serial SAL205100M2
 rack 0
!
chassis serial SAL2106055V
 rack 2
!
```

Verify the chassis configuration.

Re-pair due to Rack Removal

This task shows the automatic recalculation of the pairing algorithm when a rack is removed.

Use the following commands to check the current status of the chassis:

- **show chassis**

- **show redundancy**
- **show sdr deafult-sdr pairing**
- **show running-config chassis**

Procedure

Step 1 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters sysadmin configuration mode.

Step 2 **no chassis serial** *chassis-serial-number*

Example:

```
sysadmin-vm:F1_SC0(config)# no chassis serial  SAL205100M9
```

Removes the rack.

Step 3 **commit**

Commits the configuration changes.

Step 4 **show chassis**

Example:

```
            Serial Num    Rack Num    Rack Type   Rack State  Data Plane  Ctrl Plane
            --------------------------------------------------------------------------
            FLM213101U5   F1          FCC         OPERATIONAL CONN        CONN
            FLM213200BF   F0          FCC         OPERATIONAL CONN        CONN
            FLM213200BR   F3          FCC         OPERATIONAL CONN        CONN
            FLM21330065   F2          FCC         OPERATIONAL CONN        CONN
            SAL1834ZBRN   1           LCC         OPERATIONAL CONN        CONN
            SAL2016PB3Z   3           LCC         OPERATIONAL CONN        CONN
            SAL205100M2   0           LCC         OPERATIONAL CONN        CONN
            SAL2106055V   2           LCC         OPERATIONAL CONN        CONN
```

Verify if the removed rack details are not displayed.

Step 5 **show sdr default-sdr pairing**

Example:

```
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
```

Displays the recalculated pairing. Observe that the deleted rack is not included in the new pairing information.

Step 6 **show redundancy summary**

Example:

```
 Active Node    Standby Node
 -----------    ------------
1/RP1           2/RP0 (Node Ready, NSR:Not Configured)
1/LC0           1/LC1 (Node Ready, NSR:Not Configured)
0/RP1           1/RP0 (Node Ready, NSR:Not Configured)
3/LC0           3/LC1 (Node Ready, NSR:Not Configured)
0/RP0           3/RP1 (Node Ready, NSR:Not Configured)
2/RP1           3/RP0 (Node Ready, NSR:Ready)
0/LC0           0/LC1 (Node Ready, NSR:Not Configured)
2/LC0           2/LC1 (Node Ready, NSR:Not Configured)
```

Verify the node status and pairing.

Re-pair due to RP Insertion

When an RP is inserted to a rack to create a chassis with dual RP, the re-pairing of RPs is automatically recalculated. For more information regarding RP installation, see the *Cisco NCS 4000 Hardware Installation Guide.*

Procedure

Step 1 **show redundancy summary**

Example:

```
Active Node             Standby Node
-----------             ------------
      1/RP1           2/RP0 (Node Ready, NSR:Not Configured)
      1/LC0           1/LC1 (Node Ready, NSR:Not Configured)
      0/RP1           1/RP0 (Node Ready, NSR:Not Configured)
      3/LC0           3/LC1 (Node Ready, NSR:Not Configured)
      0/RP0           3/RP1 (Node Ready, NSR:Not Configured)
      2/RP1           3/RP0 (Node Ready, NSR:Ready)
      0/LC0           0/LC1 (Node Ready, NSR:Not Configured)
      2/LC0           2/LC1 (Node Ready, NSR:Not Configured)
```

Verify the node status and pairing.

Step 2 Insert an RP.

Step 3 **show sdr default-sdr pairing**

Example:

```
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
```

Displays the recalculated pairing. Observe that the pairing is calculated in such a way that the rack in which the new RP is installed is included.

Re-pair due to Rack Failure

A re-pair of the RPs can be initiated manually when a rack is not functional. This will re-establish rack level high availability (HA). A rack failure may occur during one or more of these circumstances:

- simultaneous hardware or software failure on both RPs in the rack
- simultaneous loss of ethernet connectivity from rest of the system on both RPs in the rack
- isolation of rack due to fiber cut(s)
- power failure

HA can be re-established by triggering re-calculation of pairing within a maintenance window. This can be done by:

- removing the affected rack from the system by deleting it from the chassis configuration using **no chassis serial** *chassis-serial-number* command.
- shutting down the rack and running re-pair manually

This section shows the steps for shutting down the rack and running the re-pair manually.

Use the following commands to check the current status of the chassis:

- **show chassis**
- **show sdr default-sdr pairing**
- **show running-config chassis**

Procedure

Step 1 **sdr default-sdr re_pair**

Example:

```
sysadmin-vm:0_RP0# sdr default-sdr re_pair
```

Removes the required rack from the re-pairing configuration.

Step 2 **show chassis**

Example:

```
Serial Num    Rack Num    Rack Type   Rack State  Data Plane  Ctrl Plane
--------------------------------------------------------------------------
FLM213101U5   F1          FCC         OPERATIONAL CONN        CONN
FLM213200BF   F0          FCC         OPERATIONAL CONN        CONN
FLM213200BR   F3          FCC         OPERATIONAL CONN        CONN
FLM21330065   F2          FCC         OPERATIONAL CONN        CONN
SAL1834ZBRN   1           LCC         OPERATIONAL CONN        CONN
SAL2016PB3Z   3           LCC         OPERATIONAL CONN        CONN
SAL205100M2   0           LCC         OPERATIONAL CONN        CONN
SAL2106055V   2           LCC         OPERATIONAL CONN        CONN
```

Verify if the newly inserted rack is visible.

Step 3 **show running-config chassis**

Example:

```
chassis serial FLM213200BF
 rack F0
!
chassis serial FLM213200BR
 rack F3
!
chassis serial FLM21330065
 rack F2
!
chassis serial SAL1834ZBRN
 rack 1
!
chassis serial SAL2016PB3Z
 rack 3
!
chassis serial SAL205100M2
 rack 0
!
chassis serial SAL2106055V
 rack 2
!
```

Verify the chassis configuration.

Step 4 **show sdr default-sdr pairing**

Example:

```
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
```

Displays the SDR algorithm. Verify if the removed rack is not included.

Re-pair due to RP Removal

This task shows how to manually initiate re-pairing when an RP is removed during the OIR procedure.

Use the following commands to check the current status of the chassis:

- **show redundancy summary**
- **show sdr default-sdr pairing**

Procedure

Step 1 Remove an RP (a part of the OIR procedure).

Step 2 **sdr default-sdr re_pair**

Example:

```
sysadmin-vm:0_RP0# sdr default-sdr re_pair
```

After an RP is removed, the pairing is impacted. This results in a mismatch between the SDR configuration and the actual state of the nodes.

Step 3 **show sdr default-sdr pairing**

Example:

```
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
```

Displays the SDR algorithm. Verify if the RP pairing is restored.

Process Placement after a Pairing Change

You must check the placement reoptimization of configuration before and after a change in pairing algorithm. This maintains High Availability (HA) for configurable processes.This includes moving to inter-rack or intra-rack pairing, running a manual re-pair, or triggering an automatic re_pair scenario. This feature provides the flexibility to decide a change in service placements based on the prediction from process placement.

Use the following commands to check the current status of the chassis:

show chassis

- **show redundancy summary**
- **show placement reoptimize**

Procedure

	Command or Action	Purpose
Step 1	**placement reoptimize** **Example:** `sysadmin-vm:0_RP0#placement reoptimize`	Reoptimizes the placement of processes to provide HA.
Step 2	**show placement reoptimize** **Example:** `sysadmin-vm:0_RP0# show placement reoptimize`	Displays predictions (if any) after reoptimizing the processes. Verify the reoptimized placement matches the current placement and no more changes are predicted.

Re-Pair RPs

Purpose	This procedure provides instructions for re-pairing route processors.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view, click the **Provisioning** > **General** > **Inter Rack Management** tabs.

The SDR Lead indicates the lead RP pair; Pairing Mode displays the pairing type.

Step 2 Select the required radio button to change the pairing type.

The RP pairs are indicated in the Pairs pane.

Step 3 Click **Refresh** to see the latest pairing after initiating re-pair.

Step 4 Click **Re-pair** to initiate re-pairing of RPs.

The table under the Pairs pane changes based on the latest re-paired RPs. Click **Re-pair** only if re-pairing is not initiated by the SDR alogirthm.

Delete RSVP File using Process Restart Command

Table 54: Feature History

Feature Name	Release Information	Feature Description
Delete RSVP File using Process Restart Command	Cisco IOS XR Release 6.5.32	The Process Restart command enables the user to delete stale RSVP files from reused Route Processors in a multi chassis (MC) system

This task describes the steps to delete the stale RSVP files.

Procedure

Step 1 **show redundancy summary**

Example:

```
Active Node    Standby Node
    -----------    ------------
          3/RP1          4/RP0 (Node Ready, NSR:Not Configured)
          4/LC0          4/LC1 (Node Ready, NSR:Not Configured)
          0/LC1          0/LC0 (Node Ready, NSR:Not Configured)
          1/RP1          2/RP0 (Node Ready, NSR:Not Configured)
          0/RP1          1/RP0 (Node Ready, NSR:Not Configured)
          5/RP1          6/RP0 (Node Ready, NSR:Not Configured)
          3/LC0          3/LC1 (Node Ready, NSR:Not Configured)
          2/RP1          3/RP0 (Node Ready, NSR:Not Configured)
          6/RP1          0/RP0 (Node Ready, NSR:Not Configured)
          1/LC1          1/LC0 (Node Ready, NSR:Not Configured)
          6/LC0          6/LC1 (Node Ready, NSR:Not Configured)
          4/RP1          7/RP0 (Node Ready, NSR:Not Configured)
          5/LC0          5/LC1 (Node Ready, NSR:Not Configured)
          5/RP0          7/RP1 (Node Ready, NSR:Ready)
          7/LC0          7/LC1 (Node Ready, NSR:Not Configured)
          2/LC0          2/LC1 (Node Ready, NSR:Not Configured)
```

Check the Active and Standby NSR pair status.

Step 2 **attach location** *Active Node ID|Standby Node ID*

Example:

```
#attach location 5/rp0
Fri Aug  6 12:35:37.129 IST
[xr-vm_node5_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:28 chkpt_rsvp_000_001_v2
#attach location 7/RP1
Fri Aug  6 12:36:12.524 IST
[xr-vm_node7_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16027648 Aug  6 12:28 chkpt_rsvp_000_001_v2
```

Check the RSVP check point file on NSR pair RPs.

Step 3 **attach location** *active-node-id|standby-node-id*

Example:

```
#attach location 0/rp0
Fri Aug  6 12:43:37.649 IST
[xr-vm_node0_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:41 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 0/rp1
Fri Aug  6 12:43:59.941 IST
[xr-vm_node0_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:41 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 1/rp0
Fri Aug  6 12:44:27.607 IST
[xr-vm_node1_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:41 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 1/rp1
Fri Aug  6 12:44:51.533 IST
[xr-vm_node1_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:41 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 2/RP0
Fri Aug  6 12:48:20.483 IST
[xr-vm_node2_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:41 chkpt_rsvp_000_001_v2
#exit
logout
```

```
#attach location 2/RP1
Fri Aug  6 12:48:53.330 IST
[xr-vm_node2_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:41 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 3/rp0
Fri Aug  6 12:49:23.656 IST
[xr-vm_node3_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:42 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 3/rp1
Fri Aug  6 12:49:39.030 IST
[xr-vm_node3_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:42 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 4/rp0
Fri Aug  6 12:50:21.691 IST
[xr-vm_node4_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:42 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 4/rp1
Fri Aug  6 12:50:47.250 IST
[xr-vm_node4_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:42 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 5/rp1
Fri Aug  6 12:51:12.117 IST
[xr-vm_node5_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:42 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 6/RP0
Fri Aug  6 12:52:22.016 IST
[xr-vm_node6_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:43 chkpt_rsvp_000_001_v2
#exit
logout
#attach location 6/RP1
Fri Aug  6 12:52:43.476 IST
[xr-vm_node6_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:43 chkpt_rsvp_000_001_v2
#exit
logout
```

```
#attach location 7/Rp0
Fri Aug  6 12:53:07.963 IST
[xr-vm_node7_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-rw-r--r-- 1 root root 16035840 Aug  6 12:43 chkpt_rsvp_000_001_v2
```

Check for stale RSVP check point file on non-NSR RPs.

Step 4 **process restart rsvp loc** *standby-node-id*

Example:

```
#process restart rsvp loc 7/RP1
```

Perform RSVP process restart on standby node.

Step 5 **attach location** *non-nsr-pair-rp-id*

Example:

```
#attach location 0/rp0
Fri Aug  6 13:01:27.675 IST
[xr-vm_node0_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 0/rp1
Fri Aug  6 13:01:57.807 IST
[xr-vm_node0_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt| grep rsvp
#exit
logout
#attach location 1/rp0
Fri Aug  6 13:02:17.709 IST
[xr-vm_node1_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 1/rp1
Fri Aug  6 13:02:35.582 IST
[xr-vm_node1_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 2/rp0
Fri Aug  6 13:03:00.773 IST
[xr-vm_node2_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 2/rp1
Fri Aug  6 13:03:18.260 IST
[xr-vm_node2_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 3/rp0
Fri Aug  6 13:03:37.685 IST
[xr-vm_node3_RP0_CPU0:~]$export PS1='#'
```

```
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 3/rp1
Fri Aug  6 13:03:51.917 IST
[xr-vm_node3_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt| grep rsvp
#exit
logout
#attach location 4/rp0
Fri Aug  6 13:04:10.322 IST
[xr-vm_node4_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 4/rp1
Fri Aug  6 13:04:24.245 IST
[xr-vm_node4_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-#exit
logout
#attach location 5/rp1
Fri Aug  6 13:05:38.152 IST
[xr-vm_node5_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 6/rp0
Fri Aug  6 13:06:00.817 IST
[xr-vm_node6_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
#exit
logout
#attach location 6/rp1
Fri Aug  6 13:06:14.616 IST
[xr-vm_node6_RP1_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
-#exit
logout
#attach location 7/RP0
Fri Aug  6 13:06:34.828 IST
[xr-vm_node7_RP0_CPU0:~]$export PS1='#'
#cd /misc/config
#ls -lrt | grep rsvp
```

Verify the stale RSVP files on the non-NSR pair RPs are deleted.

Note If any non-NSR pair RPs goes for RMA, the new card can have the stale RSVP file. When the new card is inserted, the RSVP file running on NSR pair RP does not auto-delete the stale file. After the new card insertion, when the RP card is ready, you have to perform RSVP Process Restart on the standby RP to delete the stale RSVP file.

Note During the Line Card Chassis (LCC) Rack addition, the new rack RP can have the stale RSVP files. During the migration, the RSVP files running on the NSR pair rack cannot receive notification and stale files do not delete on rack addition. After migration, you have to perform RSVP Process Restart on the standby NSR pair RPs to cleanup the stale files.

CHAPTER 54

Inter-rack Timing

This chapter provides the details about inter-rack timing in the Cisco NCS 4000 Series Router.

Introduction

In a MC system the source and destination ports of the cross connect can be across racks. Inter-rack (or cross-rack) timing allows the timing information to be passed across racks for segmentation and re-assembly needs.

Verification of Inter-rack Timing

Procedure

Step 1 Verify the inter-rack timing configuration, using command **show running-config frequency synchronization**

Example:

```
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
```

Step 2 Verify FPD Status for Timing-FPGA and ECU-FPGA, using command **show hw-module fpd** <*fpd-name*>

Example:

```
RP/2/RP0:MC_FLT+4+1#show hw-module fpd Timing-FPGA
Thu Mar 22 13:47:18.695 IST
                        FPD Versions
                      =================
Location   Card type        HWver FPD device       ATR Status   Running Programd
------------------------------------------------------------------------------
0/RP0     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82
0/RP1     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82
1/RP0     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82
```

```
1/RP1     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82
2/RP0     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82
2/RP1     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82
3/RP0     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82
3/RP1     NCS4K-RP          0.1   Timing-FPGA       S  CURRENT    3.82    3.82


RP/2/RP0:MC_FLT+4+1# show hw-module fpd ECU-FPGA
Thu Mar 22 13:47:25.868 IST
                       FPD Versions
                      =================
Location   Card type        HWver FPD device       ATR Status   Running Programd
------------------------------------------------------------------------------
0/EC0     NCS4K-ECU2        0.2   ECU-FPGA             CURRENT    4.08    4.08
1/EC0     NCS4K-ECU2        0.2   ECU-FPGA             CURRENT    4.08    4.08
2/EC0     NCS4K-ECU2        0.2   ECU-FPGA             CURRENT    4.08    4.08
3/EC0     NCS4K-ECU2        0.2   ECU-FPGA             CURRENT    4.08    4.08
RP/2/RP0:MC_FLT+4+1#
```

Step 3 Verify that all the FPDs on LC are in **CURRENT** state, using command **show hw-module location** *<LC location>* **fpd**

Example:

```
RP/2/RP0:MC_FLT+4+1# show hw-module location 0/5 fpd
                       FPD Versions
                     =================
Location   Card type        HWver FPD device       ATR Status   Running Programd
------------------------------------------------------------------------------
0/5       NCS4K-2H10T-OP-KS 0.2   Backup-ZYNQ      BSP CURRENT
0/5       NCS4K-2H10T-OP-KS 0.2   CCC-FPGA             CURRENT    1.50    1.50
0/5       NCS4K-2H10T-OP-KS 0.2   CCC-Power-On         CURRENT    1.14    1.14
0/5       NCS4K-2H10T-OP-KS 0.2   DIGI1                CURRENT    2.03    2.03
0/5       NCS4K-2H10T-OP-KS 0.2   DIGI2                CURRENT    2.03    2.03
0/5       NCS4K-2H10T-OP-KS 0.2   Ethernet-Switch      CURRENT    1.02    1.02
0/5       NCS4K-2H10T-OP-KS 0.2   GRIMA                CURRENT    1.51    1.51
0/5       NCS4K-2H10T-OP-KS 0.2   PLX-8649             CURRENT    0.11    0.11
```

Step 4 Verify Slice Manager Status for all Active LC VM's, using command **show controllers slice-control all location** *<location>*

Note Additionally verify that the Clock Status on all LCs is **External**.

Example:

```
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
```

Step 5 Verify that there are no TE alarms in the system.

Following is the list of TE alarms:

- CLOCK_PORT_STATE_CHANGE
- TIMING-PCI-ERROR
- TIMING-LOAD-ERROR
- TIMING-PLL-VAL-ERROR
- CLK-PORT-STATUS-CHNG
- TIMING-FPGA-SEU
- TE-PORT-UNAVAILABLE
- TIMING-ISOLATED-RACK

Step 6 Verify TE Port Topology, using the output of command **show controllers timing controller te-port**

a) Verify that state of all the physical links. **Link** value should be is ***Good***

Note If any of the TE Link is in **No State**, please check the physical connections.

b) Verify that the **Peer Rack** is discovered as per the topology.

c) From the **FSYNC Mastership** value, verify that only one rack converges as PRIMARY and remaining as SECONDARY.

Note FSYNC Mastership value should not be ISOLATED or SLAVE-READY or LISTENING or LEARNING.

d) Verify from the **TE state** value, that all ports (TE0-E, TE1-E, TE0-W,and TE1-W) are in FORWARDING or MASTER or BACKUP or ALTERNATE state.

e) TE State for primary rack should have value FORWARDING for all TE ports.

f) TE State for secondary rack should have values MASTER – BACKUP – FORWARDING – FORWARDING or MASTER – BACKUP – ALTERNATE – ALTERNATE for TE0-E, TE1-E, TE0-W,and TE1-W ports respectively.

g) Verify that **Delay** value is not zero.

Example:

```
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
```

Step 7 Verify Frequency Synchronization Selection Status, using the output of command **show frequency synchronization selection**

a) Verify value for SYSTEM_T0_SEL. Following are valid output combinations:

- If BITS or Frequency Synchronization source is configured then one of them should be in LOCKED state.
- If BITS or Frequency Synchronization source is not configured then the Internal Clock can be in FREERUN or HOLDOVER state.

b) Verify value for RACK<rackid>_SEL. Following are valid output combinations:

- If <rackid> is Primary Rack, then it should have either BITS or Frequency Synchronization in LOCKED state or Internal in FREERUN or HOLDOVER state.
- If <rackid> is Secondary Rack, then it should be LOCKED to TE port always..

Example:

```
RP/2/RP0:MC_FLT+4+1# show frequency synchronization selection
Thu Mar 22 11:41:09.870 IST
Node 2/RP0:
==============
Selection point: SYSTEM_T0_SEL (6 inputs, 1 selected)
  Last programmed 17:05:34 ago, and selection made 17:04:19 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : SYSTEM_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  Rack0-Bits0-In            2/RP0 RACK0_SEL 1           PRC    9  Locked
     Rack2-Bits0-In            2/RP0 RACK2_SEL 3         SSU-B    9  Available
     Internal0 [2/RP0]         2/RP0 RACK0_SEL 2           SEC  255  Available
     Internal0 [2/RP0]         2/RP0 RACK1_SEL 3           SEC  255  Available
     Internal0 [2/RP0]         2/RP0 RACK2_SEL 4           SEC  255  Available
     Internal0 [2/RP0]         2/RP0 RACK3_SEL 3           SEC  255  Available

Selection point: SYSTEM_T4_SEL (2 inputs, 1 selected)
  Last programmed 17:06:27 ago, and selection made 17:04:19 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  Rack0-Bits0-In            2/RP0 SYSTEM_T0_SEL 1       PRC    9  Locked
     Internal0 [2/RP0]         n/a                         SEC  255  Available

Selection point: RACK0_SEL (2 inputs, 2 selected)
  Last programmed 17:06:27 ago, and selection made 17:04:19 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : SYSTEM_T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  1  Rack0-Bits0-In            n/a                         PRC    9  Locked
  2  Internal0 [2/RP0]         n/a                         SEC  255  Available

Selection point: RACK1_SEL (3 inputs, 1 selected)
  Last programmed 17:05:42 ago, and selection made 17:04:59 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : SYSTEM_T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  3  Internal0 [2/RP0]         n/a                         SEC  255  Available
     1/TE0-W                   n/a                         PRC  100  Locked
     1/TE1-W                   n/a                         PRC  100  Unmonitored
```

```
Selection point: RACK2_SEL (4 inputs, 2 selected)
  Last programmed 17:05:36 ago, and selection made 17:04:24 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : SYSTEM_T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  3  Rack2-Bits0-In            n/a                       SSU-B    9  Available
  4  Internal0 [2/RP0]         n/a                         SEC  255  Available
     2/TE0-W                   n/a                         PRC  100  Locked
     2/TE1-W                   n/a                         PRC  100  Unmonitored

Selection point: RACK3_SEL (3 inputs, 1 selected)
  Last programmed 17:05:39 ago, and selection made 17:04:45 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : SYSTEM_T0_SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  3  Internal0 [2/RP0]         n/a                         SEC  255  Available
     3/TE0-E                   n/a                         PRC  100  Locked
     3/TE1-E                   n/a                         PRC  100  Unmonitored
```

Step 8 Verify the clock data table for the BITS-In or TE interfaces, using the output of command **show frequency synchronization clock-interfaces**

a) Verify that for primary or backup TE Ports, the INPUT should in UP state with proper QL Value.

b) Verify that QL Value (Quality) is not DNU.

Example:

```
RP/2/RP0:MC_FLT+4+1#show frequency synchronization clock-interfaces
Thu Mar 22 12:27:11.744 IST
  Clock interface Rack0-Bits0-In (Up - BITS 2M)
    Assigned as input for selection
    Wait-to-restore time 5 minutes
    SSM supported
    Input:
      Up
      Configured QL: Opt-I/PRC
      Effective QL: Opt-I/PRC, Priority: 9, Time-of-day Priority 100
      Supports frequency
    Output is disabled
  Next selection points: RACK0_SEL

  Clock interface Rack0-Bits0-Out (Unknown state)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: Rack0-Bits0-In
      Selected source QL: Opt-I/PRC
      Effective QL: Opt-I/PRC
  Next selection points: None

  Clock interface Rack0-Bits1-In (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: RACK0_SEL

  Clock interface Rack0-Bits1-Out (Unknown state)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: Rack0-Bits0-In
      Selected source QL: Opt-I/PRC
      Effective QL: Opt-I/PRC
  Next selection points: None

  Clock interface 0/TE0-E (Up - Inter-Chassis Sync)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: Rack0-Bits0-In
      Selected source QL: Opt-I/PRC
      Effective QL: Opt-I/PRC
  Next selection points: None

  Clock interface 0/TE1-E (Up - Inter-Chassis Sync)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: Rack0-Bits0-In
      Selected source QL: Opt-I/PRC
      Effective QL: Opt-I/PRC
  Next selection points: None

  Clock interface 0/TE0-W (Up - Inter-Chassis Sync)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: Rack0-Bits0-In
      Selected source QL: Opt-I/PRC
      Effective QL: Opt-I/PRC
  Next selection points: None

  Clock interface 0/TE1-W (Up - Inter-Chassis Sync)
    Wait-to-restore time 5 minutes
    SSM supported and enabled
    Input is disabled
    Output:
      Selected source: Rack0-Bits0-In
      Selected source QL: Opt-I/PRC
      Effective QL: Opt-I/PRC
  Next selection points: None
```

Step 9 Verify SYNCE_IN interface status using following substeps:

a) Verify that the SYNCE interfaces are not in Operationally Down State using command **show frequency synchronization interfaces brief**

Example:

```
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
```

b) Verify that the SSM packets are being sent and received using command **show frequency synchronization interfaces**

Example:

```
RP/0/RP0:MC_OTN# show frequency synchronization interfaces
Thu Mar 22 14:45:46.452 IST
Interface TenGigE0/9/0/2 (up)
  Wait-to-restore time 5 minutes
  SSM Enabled
    Peer Up for 02:24:29, last SSM received 0.717s ago
    Peer has come up 1 times and timed out 0 times
    ESMC SSMs        Total  Information     Event    DNU/DUS
      Sent:           8672         8671         1          0
      Received:       8672         8668         4       8645
  Input:
    Down - not assigned for selection
    Supports frequency
  Output:
    Selected source: Rack2-Bits0-In
    Selected source QL: Opt-I/PRC
    Effective QL: Opt-I/PRC
  Next selection points: RACK0_SEL
```

CHAPTER 55

Configure Ethernet Data Plane Loopback

This chapter describes the Cisco IOS XR commands to configure Ethernet Data Plane Loopback.

Understand Ethernet Dataplane Loopback

The Ethernet Data Plane Loopback (EDPL) feature provides a means for remotely testing the throughput of an ethernet port. User can verify the maximum rate of frame transmission with no frame loss. This feature allows both bidirectional and unidirectional throughput measurement, and on-demand/out-of-service (intrusive) operation during service turn-up. Following are the key features supported:

- This feature supports two types of ethernet loopback :
  - Facility loopback (external)—Traffic loopback occurs at the ingress interface. The traffic does not flow into the router for loopback.
  - Terminal loopback (internal)—Traffic loopback occurs at the egress interface. The traffic loopback occurs after the traffic flows into the router to the other interface.
- Ethernet loopback is supported on all the L2 transport interfaces (physical, bundle interfaces, and L2 sub-interfaces over both physical and bundle interfaces) on NCS4K-4H-OPW-QC2 line card.
- In case of bundled interface, the traffic is looped back on all the bundle link members.
- The MAC address on the looped-back traffic will always be swapped.
- Multiple filters can be applied to ensure loop back of a subset of traffic received by an interface. Supported filter qualifiers are Source MAC, Destination MAC, and VLAN priority(COS bits).

  Following are the supported combinations of filter qualifiers for external loopbacks:
  - Source MAC
  - Source MAC and Destination MAC
  - Source MAC, Destination MAC, and VLAN priority
  - Destination MAC

    - Destination MAC and VLAN priority

- Maximum number of concurrent ethernet data plane loopback sessions supported is 100.
- The default time for auto removal of an EDPL session is 5 minutes, unless explicitly specified. The session automatically stops after the time expiry.

Restrictions for Ethernet Data Plane Loopback

Following are the limitations:

- Ethernet loopback on L3 interfaces or L3 sub interfaces is not supported.
- Ethernet loopback on PW-HE is not supported.
- Following filters for loopback are not supported:
    - Outer VLAN or range of outer VLAN
    - Inner VLAN or range of inner VLAN
    - Ether Type
- Following combinations of filter qualifiers are not supported for external loopbacks:
    - Source MAC and VLAN Priority
    - VLAN Priority
- Re-write modifications on the loopback traffic is not supported.
- Simultaneous internal and external loopback on same interface is not supported.
- There shall be maximum throughput of 10Gbps for internal loopback over all the sessions.
- There is no throughput limit for external loopback sessions.
- Dropping of the packets received in the non-loopback direction is not supported.
- Loopback on multicast or broadcast MAC addresses is not supported.

Configure Ethernet Data Plane Loopback

To configure ethernet data plane loopback on an interface, perform the following steps:

Enable Ethernet Data Plane Loopback

To enable ethernet data plane loopback on an interface, perform the following steps:

Procedure

Step 1 **config**

Example:

```
RP/0/RP0:hostname# config
```

Enters the configuration mode.

Step 2 **interface** *type interface-path-id* **l2transport**

Example:

```
RP/0/RP0:hostname(config)# interface tenGigE0/1/0/1 l2transport
```

Enters the interface configuration mode.

Step 3 **ethernet loopback permit {external | internal}**

Example:

```
RP/0/RP0:hostname(config-if)# ethernet loopback permit external
```

Enables ethernet data plane loopback.

Start Ethernet Data Plane Loopback Session

To start an ethernet data plane loopback session, perform the following steps:

Procedure

Step 1 **ethernet loopback start local interface** *interface-type interface-path-id* **external source mac-address** *mac-addr* **destination mac-address** *mac-addr* **cos** *class-of-service* **timeout** *time in seconds*

Example:

```
RP/0/RP0:hostname# ethernet loopback start local interface tenGigE0/1/0/1 external source
mac-address 0000.0000.0002 destination mac-address 0000.0000.0001 cos 1 timeout 300
```

Starts an ethernet data plane loopback session.

Step 2 **show ethernet loopback active**

Example:

```
RP/0/RP0:hostname# show ethernet loopback active

Wed Apr 24 14:07:13.825 UTC
Local: TenGigE0/0/0/0, ID 2
============================================
Direction:                          External
Time out:                             0h5m0s
Time left:                           0h2m46s
Status:                               Active
Filters:
  Dot1Q:                                 Any
  Second-dot1Q:                          Any
  Source MAC Address:         0000.0000.0002
  Destination MAC Address:    0000.0000.0001
  Ethertype:                             Any
  Class of Service:                      1
```

Verifies the ethernet data plane loopback session.

Stop Ethernet Data Plane Loopback Session

To stop an ethernet data plane loopback session, perform the following steps:

Procedure

Step 1 **show ethernet loopback active**

Example:

```
RP/0/RP0:hostname# show ethernet loopback active

Wed Apr 24 14:07:13.825 UTC
Local: FortyGigE0/0/0/2, ID 1
============================================
Direction:                          External
Time out:                            1h5m0s
Time left:                           0h20m46s
Status:                               Active
Filters:
  Dot1Q:                                 Any
  Second-dot1Q:                          Any
  Source MAC Address:         0000.0000.0003
  Destination MAC Address:    0000.0000.0004
  Ethertype:                             Any
  Class of Service:                      1

Local: TenGigE0/1/0/1, ID 2
============================================
Direction:                          External
Time out:                             0h5m0s
Time left:                           0h2m46s
Status:                               Active
Filters:
  Dot1Q:                                 Any
  Second-dot1Q:                          Any
  Source MAC Address:         0000.0000.0002
  Destination MAC Address:    0000.0000.0001
  Ethertype:                             Any
  Class of Service:                      1
```

Displays all the active ethernet data plane loopback sessions. Also provides the interface details and session-id, that will be used in step2.

Step 2 **ethernet loopback stop local interface** *interface-type interface-path-id* **id** *session-id*

Example:

```
RP/0/RP0:hostname# ethernet loopback stop local interface tenGigE0/1/0/1 id 2
```

Closes the ethernet data plane loopback session.

Configuration Examples

Following are the EDPL configuration examples:

Example: Configuring external loopback on a main interface

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface TenGigE0/0/0/0 l2transport
RP/0/RP0:hostname(config-if)# encapsulation dot1q 1
RP/0/RP0:hostname(config-if)# ethernet loopback permit external
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# exit
RP/0/RP0:hostname# ethernet loopback start local interface tenGigE0/0/0/0 external source
mac-address 0000.0000.0002 destination mac-address 0000.0000.0001 cos 1 timeout 300
```

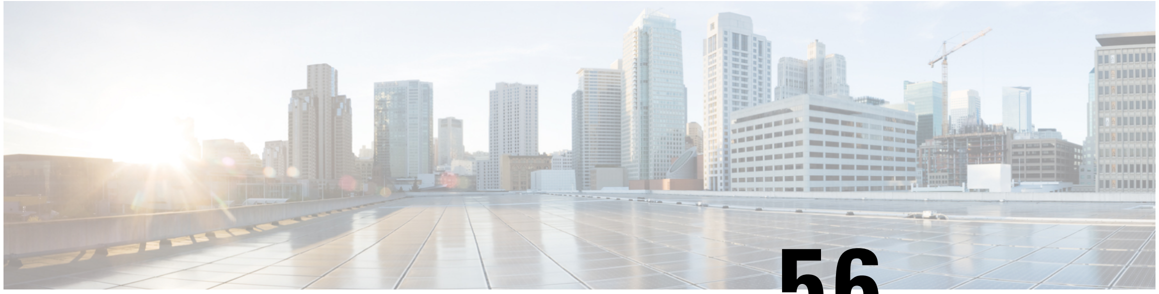
Example: Configuring internal loopback on a sub interface

```
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# interface FortyGigE0/4/0/2.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 1
RP/0/RP0:hostname(config-subif)# ethernet loopback permit internal
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# exit
RP/0/RP0:hostname# ethernet loopback start local interface FortyGigE0/4/0/2.1 external
source mac-address 0000.0000.0008 destination mac-address 0000.0000.0009 cos 1 timeout 300
```

Example: Configuring EDPL for internal loopback session on bundle sub interface

```
Topology:
(4/20)Tg1——(0/2/0/0/1)CE1(0/2/0/0/2)———(0/3/0/0/2)PE1(0/3/0/0/3)———(0/7/0/0/3)PE2(TenGigE0/7/0/0/4)———(TenGigE0/2/0/0/2)
 CE2 (Te0/2/0/0/1)------Tg2(4/17)

Config CE1
==========
RP/0/RP0:hostname# configure
RP/0/RP0:hostname(config)# interface Bundle-Ether1
RP/0/RP0:hostname(config-if)# bundle maximum-active links 1 hot-standby
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 1
RP/0/RP0:hostname(config-subif)# ethernet loopback
RP/0/RP0:hostname(config-subif)#   permit internal
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# xconnect group VPWS1
RP/0/RP0:hostname(config-l2vpn-xc)# p2p p1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface TenGigE0/2/0/0/1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# exit
RP/0/RP0:hostname(config-l2vpn-xc)#exit
RP/0/RP0:hostname(config-l2vpn)#exit
RP/0/RP0:hostname(config)# interface TenGigE0/2/0/0/1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 1
RP/0/RP0:hostname(config-subif)# exit
```

```
Config PE1
===========
RP/0/RP0:hostname(config)# interface Bundle-Ether1
RP/0/RP0:hostname(config-if)# bundle maximum-active links 1 hot-standby
RP/0/RP0:hostname(config-if)# exit
RP/0/RP0:hostname(config)# interface Bundle-Ether1.1 l2transport
RP/0/RP0:hostname(config-subif)# encapsulation dot1q 1
RP/0/RP0:hostname(config-subif)# exit
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# pw-class vpws1
RP/0/RP0:hostname(config-l2vpn-pwc)# encapsulation mpls
RP/0/RP0:hostname(config-l2vpn-pwc)# exit
RP/0/RP0:hostname(config-l2vpn)# xconnect group VPWS1
RP/0/RP0:hostname(config-l2vpn-xc)# p2p p1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface Bundle-Ether1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# neighbor ipv4 22.22.22.22 pw-id 1
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class vpws1
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# exit
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# exit
RP/0/RP0:hostname(config-l2vpn-xc)# exit
RP/0/RP0:hostname(config-l2vpn)# exit


Config CE2
==========
RP/0/RP0:hostname(config)# interface Bundle-Ether1.1 l2transport
RP/0/RP0:hostname# encapsulation dot1q 1
RP/0/RP0:hostnameconfig-subif)# exit
RP/0/RP0:hostname(config)# l2vpn
RP/0/RP0:hostname(config-l2vpn)# pw-class vpws1
RP/0/RP0:hostname(config-l2vpn-pwc)# encapsulation mpls
RP/0/RP0:hostname(config-l2vpn-pwc)# exit
RP/0/RP0:hostname(config-l2vpn)# xconnect group VPWS1
RP/0/RP0:hostname(config-l2vpn-xc)# p2p p1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# interface TenGigE0/2/0/0/1.1
RP/0/RP0:hostname(config-l2vpn-xc-p2p)#  neighbor ipv4 2.2.2.2 pw-id 1
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# pw-class vpws1
RP/0/RP0:hostname(config-l2vpn-xc-p2p-pw)# exit
RP/0/RP0:hostname(config-l2vpn-xc-p2p)# exit
RP/0/RP0:hostname(config-l2vpn-xc)# exit
RP/0/RP0:hostname(config-l2vpn)# exit
RP/0/RP0:hostname(config-l2vpn)# exit

RP/0/RP0:hostname# ethernet loopback start local  Bundle-Ether1 internal timeout none
```



CHAPTER 56

Configure Zero Touch Provisioning

This chapter describes Zero Touch Provisioning (ZTP) and procedures to configure ZTP.

Table 55: Feature History

Feature Name	Release Information	Feature Description
Zero Touch Provisioning (ZTP)	Cisco IOS XR Release 6.5.31	ZTP allows you to easily deploy the network with minimal user intervention. You need not login to each router to configure the router during the network deployment. Two ZTP configurations are supported: • ZTP client runs on 42XX platform (XE Device) and ZTP is configured on NCS 4000 • ZTP client runs on NCS 540 and ZTP is configured on NCS 4000 Commands added: • ztp initiate • ztp terminate • ztp clean

Understanding ZTP

ZTP makes it easier for the network operators to deploy and manage the network. The field technician need not login into each router during its deployment to configure the router as it is automatically configured.

ZTP Client on 42XX platform (XE Device)

ZTP client runs on the 42XX platform and ZTP is configured on NCS 4000. In this case, the ZTP client uses the TFTP server to download and apply an initial ZTP configuration.

ZTP Client on NCS 540

ZTP client runs on NCS 540 and ZTP is configured on NCS 4000. In this case, the ZTP client uses the HTTP server to perform the following tasks:

- Download and apply an initial configuration—If the downloaded file content starts with **!! IOS XR** it is considered as a configuration file, and ZTP performs **apply_config** action on the configuration file.
- Download and execute a shell script—If the downloaded file content starts with **#! /bin/bash**, **#! /bin/sh** or **#!/usr/bin/python** it is considered as a script file, and ZTP executes the script.

Prerequisites

- The connection between the DHCP server, TFTP (for 42XX platform) or HTTP server (for NCS 540), and the router must be established.
- The TFTP or HTTP server must have the required ZTP configuration file and must be accessible to the router.
- (ZTP on NCS 540) Ensure that the ncs4k-k9sec.pkg and ncs4k-mgbl.pkg packages are installed on NCS 4000.
- (ZTP on NCS 540) Ensure that the host name is not configured on NCS 540.

Restriction

ZTP is supported only on the data port and not on the management port.

Limitation of ZTP on NCS 540

ZTP client does not run on NCS 540 when the DHCP sever is configured on a VLAN other than the default VLAN.

Example of ZTP Configuration on NCS 4000 to run ZTP on NCS 540

Note Place the configuration file in the http home directory on the http server. If the http server is configured on NCS 4000, then the configuration file must be placed under the **/pkg/CTC** directory on NCS 4000.

Example

```
pool vrf default ipv4 test_pool
 network 20.0.0.0/24
 exclude 20.0.0.0 0.0.0.0
 exclude 20.0.0.1 0.0.0.0
 exclude 20.0.0.2 0.0.0.0
 exclude 20.255.255.255 0.0.0.0
!
dhcp ipv4
 profile test_dhcp server
  bootfile http://20.0.0.1/ncs5k-day0.cfg
  pool test_pool
  option 43 hex 010a6578722d636f6e666967020100
  default-router 20.0.0.1
 !
 interface FortyGigE0/8/0/7 server profile test_dhcp
!
interface FortyGigE0/8/0/7
 ipv4 address 20.0.0.1 255.255.255.0
!
http server
!
```

Start ZTP on NCS 540

There are two modes of ZTP.

- Fresh boot
- Manual invocation

Fresh Boot

Perform the following steps to perform fresh boot using ZTP.

1. Trigger ZTP after reload to download and execute a config file or a script.
   a. Change the order of fetcher priority in **/pkg/etc/ztp.ini** file as follows.

```
[ios:~]$ cat /pkg/etc/ztp.ini
[Fetcher Priority]
usb:    0
DPort4: 1
Mgmt4:  2
Mgmt6:  3
```

```
DPort6: 4
[ios:~]$
```

b. Use the **conf t/commit replace** command.

c. Use the **ztp clean** command.

d. Use the **reload location all** command.

or

Use the **hw-module location all reload** command in admin console.

You can monitor the console logs available at **/disk0:/ztp/ztp.log** to check the status of the ZTP operation.

2. Trigger ZTP after reload to download and execute a config file or a script and also to upgrade device image using iPXE.

a. Change the order of fetcher priority in **/pkg/etc/ztp.ini** file as follows.

```
[ios:~]$ cat /pkg/etc/ztp.ini
[Fetcher Priority]
usb:    0
DPort4: 1
Mgmt4:  2
Mgmt6:  3
DPort6: 4
[ios:~]$
```

b. Use the **hw-module location all bootmedia network reload** command in admin console.

You can monitor the console logs available at **/disk0:/ztp/ztp.log** to check the status of the ZTP operation.

Manual Invocation

Perform the following steps to manually initiate ZTP.

1. Perform the following steps to manually initiate ZTP on a data interface.

a. Unconfigure host name on the router.

b. Use the **ztp initiate debug verbose int** *data interface-name* command.

You can monitor the console logs available at **/disk0:/ztp/ztp.log** to check the status of the ZTP operation.

2. Perform the following steps to manually initiate ZTP on all the data interfaces.

a. Unconfigure host name on the router.

b. Use the **ztp initiate dataport dhcp4 noprompt** command.

You can monitor the console logs available at **/disk0:/ztp/ztp.log** to check the status of the ZTP operation.

Terminate ZTP Sessions in Progress

Use the **ztp terminate** command to terminate any ZTP session in progress.

Remove ZTP State Files

Use the **ztp clean** command to remove the ZTP state files.

ZTP Script

The following is the example content of **/pkg/CTC/ztp_day0.sh** script.

```
ztp_day0.sh

#!/bin/bash
source /pkg/bin/ztp_helper.sh

# If we want to only run one time:
xrcmd "show running" | grep -q myhostname
if [[ $? -eq 0 ]]; then
    echo Already configured
fi

#set the hostname
xrapply_string_with_reason "system renamed again" "hostname venus"
```

ZTP Utilities

ZTP includes a set of shell utilities that can be sourced within the user script. **ztp_helper.sh** is a shell script that can be sourced by the user script. **ztp_helper.sh** provides simple utilities to access some XR functionalities. Following are the bash functions that can be invoked:

- **xrcmd**—Used to run a single XR exec command:

  ```
  xrcmd “show running”
  ```

- **xrapply**—Applies the block of configuration, specified in a file:

  ```
  cat >/tmp/config <<%%
  !! XR config example
  hostname node1-mgmt-via-xrapply
  %%
  xrapply /tmp/config
  ```

- **xrapply_with_reason**—Used to apply a block of XR configuration along with a reason for logging purpose:

  ```
  cat >/tmp/config <<%%
  !! XR config example
  hostname node1-mgmt-via-xrapply
  %%
  xrapply_with_reason "this is a system upgrade" /tmp/config
  ```

- **xrapply_string**—Used to apply a block of XR configuration in one line:

  ```
  xrapply_string "hostname foo\ninterface GigabitEthernet0/0/0/0\nipv4 address 1.2.3.44
  255.255.255.0\n"
  ```

- **xrapply_string_with_reason**—Used to apply a block of XR configuration in one line along with a reason for logging purposes:

  ```
  xrapply_string_with_reason ”system renamed again" "hostname venus\n interface
  TenGigE0/0/0/0\n ipv4 address 172.30.0.144/24\n”
  ```

- **xrreplace**—Used to apply XR configuration replace in XR namespace through a file.

```
cat rtr.cfg <<%%
!! XR config example
hostname node1-mgmt-via-xrreplace
%%
xrreplace rtr.cfg
```

- **admincmd**—Used to run an admin CLI command in XR namespace. Logs can be found in **/disk0:/ztp/ztp_admincmd.log**

```
admincmd running [show platform]
```

- **xrapply_with_extra_auth**—Used to apply XR configuration that requires authentication, in XR namespace through a file. The **xrapply_with_extra_auth** API is used when configurations that require additional authentication to be applied such as alias, flex groups.

```
cat >/tmp/config <<%%
!! XR config example
alias exec alarms show alarms brief system active
alias exec version run cat /etc/show_version.txt
%%
xrapply_with_extra_auth >/tmp/config
```

- **xrreplace_with_extra_auth**—Used to apply XR configuration replace in XR namespace through a file The **xrreplace_with_extra_auth** API is used when configurations that require additional authentication to be applied such as alias, flex groups.

```
cat >/tmp/config <<%%
!! XR config example
alias exec alarms show alarms brief system active
alias exec version run cat /etc/show_version.txt
%%
xrreplace_with_extra_auth >/tmp/config
```

Example of ZTP Configuration on NCS 4000 to run ZTP on 42XX Platform

Note Place the configuration file in the tftp home directory on the tftp server.

Before You Begin

Before testing ZTP, set the configuration register on 42XX platform to 0x2

```
Router#configure terminal
Router(config)#config
Router(config)#config-register 0x2
Router(config)#end
```

The configuration register can be viewed by using the **show version** command.

Example

```
tftp vrf ZTP ipv4 server homedir disk1:/config access-list ztp
!
vrf ZTP
 rd 1111:1111
 address-family ipv4 unicast
 !
!
pool vrf ZTP ipv4 test_pool
 network 209.165.201.0/27
 exclude 209.165.201.0 0.0.0.0
 exclude 209.165.201.1 0.0.0.0
 exclude 209.165.201.2 0.0.0.0
 exclude 209.165.201.30 0.0.0.0
!
dhcp ipv4
 profile test_dhcp server
  match option 60 string "ciscopnp" action allow
  match option 60 default action drop
  bootfile xe-device.cfg
  pool test_pool
  secure-arp
  option 150 ip 209.165.201.1
  default-router 209.165.201.1
 !
 interface TenGigE0/8/0/1/3.1111 server profile test_dhcp
!
ipv4 access-list ztp
 10 permit ipv4 209.165.201.0 0.0.0.255 any
!
interface TenGigE0/8/0/1/3.1111
 vrf ZTP
 ipv4 address 209.165.201.1 255.255.255.0
 encapsulation dot1q 1111
!
```

Start ZTP on 42XX platform

ZTP is started when the router boots up without configuration in NVRAM. This can be achieved using one of the following methods:

- Press the ZTP button located on the front panel for about two seconds. Pressing the ZTP button for about eight seconds reloads the router. ZTP is not started in this case.
- Use the **write erase** command on the router and reload it without saving the configurations.

CHAPTER 57

Implement LPTS

LPTS Overview

Local Packet Transport Services (LPTS) maintains tables describing all packet flows destined for the secure domain router (SDR), making sure that packets are delivered to their intended destinations.

LPTS uses two components to accomplish this task: the port arbitrator and flow managers. The port arbitrator and flow managers are processes that maintain the tables that describe packet flows for a logical router, known as the Internal Forwarding Information Base (IFIB). The IFIB is used to route received packets to the correct Route Processor for processing.

LPTS interfaces internally with all applications that receive packets from outside the router. LPTS functions without any need for customer configuration. However, the policer values can be customized if necessary. The LPTS show commands are provided that allow customers to monitor the activity and performance of LPTS flow managers and the port arbitrator.

LPTS Policers

In Cisco IOS XR, the control packets, which are destined to the Route Processor (RP), are policed using a set of ingress policers in the incoming ports. These policers are programmed statically during bootup by LPTS components. The policers are applied based on the flow type of the incoming control traffic. The flow type is determined by looking at the packet headers. The policer rates for these static ingress policers are defined in a configuration file, which are programmed on the route processor during bootup. You can change the policer values based on the flow types of these set of ingress policers. You are able to configure the rate per policer per node.

Note

- You can get the default policer values and the current rates of the flow types from the output of the following show command:

```
show lpts pifib hardware police
```

Configuration Example

Configure the LPTS policer for the OSPF and BGP flow types with the following values globally for all nodes:

- ospf unicast default rate 3000
- bgp default rate 4000

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#lpts pifib hardware police
RP/0/RP0:hostname(config-pifib-policer-global)#flow ospf unicast default rate 3000
RP/0/RP0:hostname(config-pifib-policer-global)#flow bgp default rate 4000
RP/0/RP0:hostname (config-pifib-policer-global)#commit
```

Running Configuration

```
lpts pifib hardware police
flow ospf unicast default rate 3000
flow bgp default rate 4000
!
```

Verification

```
RP/0/RP0:hostname#show run lpts pifib hardware police
lpts pifib hardware police
flow ospf unicast default rate 3000
flow bgp default rate 4000
```

Configuration Example

Configure the LPTS policer for the OSPF and BGP flow types with the following values on an individual node - 0/0/CPU0:

- ospf unicast default rate 3000
- flow bgp default rate 4000

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#lpts pifib hardware police location 0/0/CPU0
RP/0/RP0:hostname(config-pifib-policer-per-node)#flow ospf unicast default rate 3000
RP/0/RP0:hostname(config-pifib-policer-per-node)#flow bgp default rate 4000
RP/0/RP0:hostname(config-pifib-policer-per-node)#commit
```

Running Configuration

```
lpts pifib hardware police location 0/0/CPU0
flow ospf unicast default rate 3000
flow bgp default rate 4000
```

Verification

The **show lpts pifib hardware police location 0/0/CPU0** command displays pre-Internal Forwarding Information Base (IFIB) information for the designated node.

```
RP/0/RP0:hostname#show lpts pifib hardware police location 0/0/CPU0
------------------------------------------------------------
                Node 0/0/CPU0:
-------------------------------------------------------------
 Burst = 100ms for all flow types
-------------------------------------------------------------
FlowType               Policer Type    Cur. Rate Burst     npu
---------------------- ------- ------- --------- --------- ---------
OSPF-uc-default        32106   np      3000      1000      0
BGP-default            32118   np      4000      1250      0
```

Verification

The **show controllers npu stats traps-all instance all location 0/0/CPU0** command displays packets that are locally processed and packets that are dropped by the CPU.

```
RP/0/RP0:hostname# show controllers npu stats traps-all instance all location 0/0/CPU0

Trap Type                                   NPU  Trap TrapStats   Policer Packet    Packet

                                            ID    ID      ID             Accepted  Dropped
==========================================================================================
RxTrapMimSaMove(CFM_DOWM_MEP_DMM)             0    6    0x6         32037   0         0

RxTrapMimSaUnknown(RCY_CFM_DOWN_MEP_DMM)      0    7    0x7         32037   0         0

RxTrapAuthSaLookupFail (IPMC default)         0    8    0x8         32033   0         0

RxTrapSaMulticast                             0    11   0xb         32018   0         0

RxTrapArpMyIp                                 0    13   0xd         32001   0         0

RxTrapArp                                     0    14   0xe         32001   11        0

RxTrapDhcpv4Server                            0    18   0x12        32022   0         0

RxTrapDhcpv4Client                            0    19   0x13        32022   0         0

RxTrapDhcpv6Server                            0    20   0x14        32022   0         0

RxTrapDhcpv6Client                            0    21   0x15        32022   0         0

RxTrapL2Cache_LACP                            0    23   0x17        32003   0         0

RxTrapL2Cache_LLDP1                           0    24   0x18        32004   0         0

RxTrapL2Cache_LLDP2                           0    25   0x19        32004   1205548   0

RxTrapL2Cache_LLDP3                           0    26   0x1a        32004   0         0

RxTrapL2Cache_ELMI                            0    27   0x1b        32005   0         0

RxTrapL2Cache_BPDU                            0    28   0x1c        32027   0         0

RxTrapL2Cache_BUNDLE_BPDU                     0    29   0x1d        32027   0         0

RxTrapL2Cache_CDP                             0    30   0x1e        32002   0         0

RxTrapHeaderSizeErr                           0    32   0x20        32018   0         0
```

```
RxTrapIpCompMcInvalidIp                   0    35   0x23        32018   0          0
RxTrapMyMacAndIpDisabled                  0    36   0x24        32018   0          0
RxTrapMyMacAndMplsDisable                 0    37   0x25        32018   0          0
RxTrapArpReply                            0    38   0x26        32001   2693       0
RxTrapFibDrop                             0    41   0x29        32018   0          0
RxTrapMTU                                 0    42   0x2a        32020   0          0
RxTrapMiscDrop                            0    43   0x2b        32018   0          0
RxTrapL2AclDeny                           0    44   0x2c        32034   0          0
Rx_UNKNOWN_PACKET                         0    46   0x2e        32018   0          0
RxTrapL3AclDeny                           0    47   0x2f        32034   0          0
RxTrapOamY1731MplsTp(OAM_SWOFF_DN_CCM)    0    57   0x39        32029   0          0
RxTrapOamY1731Pwe(OAM_SWOFF_DN_CCM)       0    58   0x3a        32030   0          0
RxTrapOamLevel                            0    64   0x40        32023   0          0
RxTrapRedirectToCpuOamPacket              0    65   0x41        32025   0          0
RxTrapOamPassive                          0    66   0x42        32024   0          0
RxTrap1588                                0    67   0x43        32038   0          0
RxTrapExternalLookupError                 0    72   0x48        32018   0          0
RxTrapArplookupFail                       0    73   0x49        32001   0          0
RxTrapUcLooseRpfFail                      0    84   0x54        32035   0          0
RxTrapMplsControlWordTrap                 0    88   0x58        32015   0          0
RxTrapMplsControlWordDrop                 0    89   0x59        32015   0          0
RxTrapMplsUnknownLabel                    0    90   0x5a        32018   0          0
RxTrapIpv4VersionError                    0    98   0x62        32018   0          0
RxTrapIpv4ChecksumError                   0    99   0x63        32018   0          0
RxTrapIpv4HeaderLengthError               0    100  0x64        32018   0          0
RxTrapIpv4TotalLengthError                0    101  0x65        32018   0          0
RxTrapIpv4Ttl0                            0    102  0x66        32008   0          0
RxTrapIpv4Ttl1                            0    104  0x68        32008   0          0
RxTrapIpv4DipZero                         0    106  0x6a        32018   0          0
RxTrapIpv4SipIsMc                         0    107  0x6b        32018   0          0
RxTrapIpv6VersionError                    0    109  0x6d        32018   0          0
RxTrapIpv6HopCount0                       0    110  0x6e        32011   0          0
```

```
RxTrapIpv6LoopbackAddress                     0    113  0x71       32018   0          0
RxTrapIpv6MulticastSource                     0    114  0x72       32018   0          0
RxTrapIpv6NextHeaderNull                      0    115  0x73       32010   0          0
RxTrapIpv6Ipv4CompatibleDestination           0    121  0x79       32018   0          0
RxTrapMplsTtl1                                0    125  0x7d       32012   316278     2249
RxTrapUcStrictRpfFail                         0    137  0x89       32035   0          0
RxTrapMcExplicitRpfFail                       0    138  0x8a       32033   0          0
RxTrapOamp(OAM_BDL_DN_NON_CCM)                0    141  0x8d       32031   0          0
RxTrapOamEthUpAccelerated(OAM_BDL_UP_NON_CCM) 0    145  0x91       32032   0          0
RxTrapReceive                                 0    150  0x96       32017   125266112  0
RxTrapUserDefine_FIB_IPV4_NULL0               0    151  0x97       32018   0          0
RxTrapUserDefine_FIB_IPV6_NULL0               0    152  0x98       32018   0          0
RxTrapUserDefine_FIB_IPV4_GLEAN               0    153  0x99       32016   0          0
RxTrapUserDefine_FIB_IPV6_GLEAN               0    154  0x9a       32016   0          0
RxTrapUserDefine_IPV4_OPTIONS                 0    155  0x9b       32006   0          0
RxTrapUserDefine_IPV4_RSVP_OPTIONS            0    156  0x9c       32007   0          0
RxTrapUserDefine                              0    157  0x9d       32026   0          0
RxTrapUserDefine_BFD                          0    163  0xa3       32028   0          0
RxTrapMC                                      0    181  0xb5       32033   0          0
RxNetflowSnoopTrap0                           0    182  0xb6       32018   0          0
RxNetflowSnoopTrap1                           0    183  0xb7       32018   0          0
RxTrapMimSaMove(CFM_DOWM_MEP_DMM)             1    6    0x6        32037   0          0
RxTrapMimSaUnknown(RCY_CFM_DOWN_MEP_DMM)      1    7    0x7        32037   0          0
RxTrapAuthSaLookupFail (IPMC default)         1    8    0x8        32033   0          0
RxTrapSaMulticast                             1    11   0xb        32018   0          0
RxTrapArpMyIp                                 1    13   0xd        32001   0          0
```

Associated Commands

- lpts pifib hardware police
- flow ospf
- flow bgp
- show lpts pifib hardware police

Per Port Rate Limiting of Multicast and Broadcast Punt Packets

This feature enables rate limiting of multicast and broadcast punted traffic at the interface level. Currently, a rate limit is supported per NPU level. This feature supports rate limiting at the interface level so as to protect a port from receiving the multicast and broadcast storm of punted traffic. Rate limiting for all the L3 protocol punt packets and L2 protocol packets (only ERPS, and DOT1x) is supported on physical and bundle main interfaces.

Configuring a Rate Limit to the Multicast and Broadcast Punted Traffic

You can configure the multicast and broadcast rate limit in three levels:

- Interface level
- Global level
- Domain level

Along with rate limiting the multicast and broadcast punted traffic, you can configure rate limit to these protocol punted traffic:

- ARP
- CDP
- LACP

The protocol specific configurations are explained in the below section.

Limitation

When broadcast and multicast rate limit is configured along with ARP rate limit, the ARP packets increment broadcast and multicast counters.

Interface Level

This example shows how to configure the rate limit of 1000 pps for the multicast and broadcast punted traffic at the TenGig interface:

Note A interface level rate limit configuration has the highest priority over a global and domain level configurations.

1. `RP/0/RP0:hostname# configure`

   Enters the configuration mode.

2. `RP/0/RP0:hostname(config)# lpts punt police`

   Enters punt configuration mode.

3. `RP/0/RP0:hostname(config-lpts-punt-policer)#  interface TenGigE0/0/0/8/0`

   Enters per interface level policer configuration.

4.
```
RP/0/RP0:hostname(config-lpts-punt-policer-global-if)#  mcast rate 1000
```
Configures a rate limit of 1000 pps for multicast punted traffic.

5.
```
RP/0/RP0:hostname(config-lpts-punt-policer-global-if)#  bcast rate 1000
```
Configures a rate limit of 1000 pps for broadcast punted traffic.

6.
```
RP/0/RP0:hostname(config-lpts-punt-policer-global-if)#  commit
```
Commit the configuration.

Global Level

This example shows how to configure the rate limit of:

- 1000 pps for the multicast and broadcast punted traffic

1.
```
RP/0/RP0:hostname# configure
```
Enters the configuration mode.

2.
```
RP/0/RP0:hostname(config)# lpts punt police
```
Enters punt configuration mode.

3.
```
RP/0/RP0:hostname(config-punt-policer-global)# mcast rate 1000
```
Configures multicast rate limit of 1000 pps.

4.
```
RP/0/RP0:hostname(config-punt-policer-global)# bcast rate 1000
```
Configures broadcast rate limit of 1000 pps.

5.
```
RP/0/RP0:hostname(config-punt-policer-global)# commit
```
Commit the configuration.

Domain Level

This example shows how to configure the LPTS domain and apply a rate limit of:

- 1000 pps for the multicast and broadcast punted traffic

1.
```
RP/0/RP0:hostname# configure
```
Enters the configuration mode.

2.
```
RP/0/RP0:hostname(config)# lpts punt police domain ACCESS
```
Enters LPTS punt domain configuration mode.

3.
```
RP/0/RP0:hostname(config-lpts-punt-policer-global-ACCESS)# mcast 5000
```
Configures multicast rate limit of 5000 pps.

4.
```
RP/0/RP0:hostname(config-lpts-punt-policer-global-ACCESS)# bcast 5000
```
Configures broadcast rate limit of 5000 pps.

5.
```
RP/0/RP0:hostname(config-lpts-punt-policer-global-ACCESS)# exit
```
Exits the domian ACCESS mode.

6.
   ```
   RP/0/RP0:hostname(config-lpts-punt-policer)# exit
   ```
   Exits the LPTS punt configuration mode.

7.
   ```
   RP/0/RP0:hostname(config)# lpts pifib hardware domain ACCESS
   ```
   Enters LPTS hardware domain configuration mode.

8.
   ```
   RP/0/RP0:hostname(config-pifib-domain-ACCESS)# interface TenGigE0/0/0/8/1
   ```
   Applies the domian ACCESS to the TenGigE0/0/0/8/1 interface node.

9.
   ```
   RP/0/RP0:hostname(config-pifib-domain-ACCESS)# exit
   ```
   Exits LPTS domain mode.

10.
    ```
    RP/0/RP0:hostname(config)# lpts punt police location 0/0/CPU0
    ```
    Enters LPTS punt police configuration mode.

11.
    ```
    RP/0/RP0:hostname(config-lpts-punt-policer)# protocol arp rate 500
    ```
    Configures the rate limit of 500 pps for the ARP protocol packets.

12.
    ```
    RP/0/RP0:hostname(config-lpts-punt-policer)# protocol cdp rate 500
    ```
    Configures the rate limit of 500 pps for the CDP protocol packets.

13.
    ```
    RP/0/RP0:hostname(config-lpts-punt-policer)# exit
    ```
    Exits the LPTS punt policer configuration mode.

14.
    ```
    RP/0/RP0:hostname(config)# lpts punt police location 0/4/CPU0
    ```
    Configures LPTS punt police at the node location 0/4/CPU0.

15.
    ```
    RP/0/RP0:hostname(config)# commit
    ```
    Commits the configuration

Note After committing the configuration, verify if an error message is captured in the syslog with respect to the multicast and broadcast rate limit.

Protocol Punted Traffic

You can configure a rate limit to these protocol punted traffic - ARP, CDP, and LACP.

This example shows how to configure the following rate limit for protocol punted traffic at the global level:

- 500 pps for ARP and CDP protocols

1.
   ```
   RP/0/RP0:hostname(config-punt-policer-global)# protocol arp rate 500
   ```
   Configures rate limit of 500 pps for protocol ARP packets.

2.
   ```
   RP/0/RP0:hostname(config-punt-policer-global)# protocol cdp rate 500
   ```
   Configures rate limit of 500 pps for protocol CDP packets.

3.
   ```
   RP/0/RP0:hostname(config-punt-policer-global)# commit
   ```

Commit the configuration.

This example shows how to configure the following rate limit for protocol punted traffic at the domain level:

- 500 pps for ARP and CDP protocols

1. `RP/0/RP0:hostname(config)# lpts pifib hardware domain ACCESS`

   Enters LPTS hardware domain configuration mode.

2. `RP/0/RP0:hostname(config-pifib-domain-ACCESS)# interface TenGigE0/0/0/8/1`

   Applies the domian ACCESS to the TenGigE0/0/0/8/1 interface node.

3. `RP/0/RP0:hostname(config-pifib-domain-ACCESS)# exit`

   Exits LPTS domain mode.

4. `RP/0/RP0:hostname(config)# lpts punt police location 0/0/CPU0`

   Enters LPTS punt police configuration mode.

5. `RP/0/RP0:hostname(config-lpts-punt-policer)# protocol arp rate 500`

   Configures the rate limit of 500 pps for the ARP protocol packets.

6. `RP/0/RP0:hostname(config-lpts-punt-policer)# protocol cdp rate 500`

   Configures the rate limit of 500 pps for the CDP protocol packets.

7. `RP/0/RP0:hostname(config-lpts-punt-policer)# exit`

   Exits the LPTS punt policer configuration mode.

8. `RP/0/RP0:hostname(config)# lpts punt police location 0/4/CPU0`

   Configures LPTS punt police at the node location 0/4/CPU0.

9. `RP/0/RP0:hostname(config)# commit`

   Commits the configuration

Running Config

```
lpts punt police
 interface TenGigE0/0/0/8/0
  mcast rate 1000
  bcast rate 1000
 !
 mcast rate 1000
 bcast rate 1000
 protocol arp rate 700
 protocol cdp rate 700
 domain ACCESS
  mcast rate 5000
  bcast rate 5000
 !
!
lpts pifib hardware domain ACCESS
 interface TenGigE0/0/0/8/1
!
lpts punt police location 0/0/CPU0
 protocol arp rate 500
 protocol cdp rate 500
```

```
!
lpts punt police location 0/4/CPU0
!
```

Verification

In the below show command output, you should look for highlighted fields that confirms the rate limit configuration at domain, and interface level:

```
RP/0/RP0:hostname# show lpts punt statistics location 0/0/CPU0
Fri Nov 15 06:23:20.410 UTC

 Lpts Punt Policer Statistics:
 -----------------------------
 Punt_Reason  - Ingress Packets type to be Punt policed
 Scope        - Configured scope - Global/Domain/IFH
 State        - Current config state
 Rate         - Policer rate in PPS
 Accepted     - No of Packets Accepted
 Dropped      - No of Packets Dropped
 Domain       - Domain name

----------------------------------------------------
Interface Name      : any
Punt Reason         : ARP
Domain              : ACCESS
Scope               : Default
State               : Active
Configured Rate     : 1000
Operational Rate    : 986
Accepted            : 0
Dropped             : 0
Last Update (if any):
Punt Type           : ARP
Interface Handle    : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate         : 1000
Domain              : 1
CreateTime          : Fri Nov 15 2019 06:22:42.237.188
Platform:
  PolicerID   : 32398
  NPU: TCAM-entry    StatsID
    0:        172 0x80001d54
    1:        297 0x80001dd0
    2:        172 0x80001d54
    3:        172 0x80001d54
    4:        172 0x80001d54
    5:        172 0x80001d54
----------------------------------------------------
Interface Name      : any
Punt Reason         : CDP
Domain              : ACCESS
Scope               : Default
State               : Active
Configured Rate     : 1000
Operational Rate    : 986
Accepted            : 0
Dropped             : 0
Last Update (if any):
Punt Type           : CDP
Interface Handle    : 0x00000000
```

```
Is Virtual          : 0
Is Enabled          : 1
Packet Rate         : 1000
Domain              : 1
CreateTime          : Fri Nov 15 2019 06:22:42.258.192
Platform:
  PolicerID   : 32404
  NPU: TCAM-entry    StatsID
    0:        173 0x80001d55
    1:        298 0x80001dd1
    2:        173 0x80001d55
    3:        173 0x80001d55
    4:        173 0x80001d55
    5:        173 0x80001d55
----------------------------------------------------
Interface Name      : any
Punt Reason         : ARP
Domain              : default
Scope               : Local
State               : Active
Configured Rate     : 500
Operational Rate    : 515
Accepted            : 980
Dropped             : 0
Last Update (if any):
Punt Type           : ARP
Interface Handle    : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate         : 500
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:31:25.136.800
Platform:
  PolicerID   : 32306
  NPU: TCAM-entry    StatsID
    0:         41 0x80001cd2
    1:         41 0x80001cd2
    2:         41 0x80001cd2
    3:         41 0x80001cd2
    4:         41 0x80001cd2
    5:         41 0x80001cd2
----------------------------------------------------
Interface Name      : any
Punt Reason         : CDP
Domain              : default
Scope               : Local
State               : Active
Configured Rate     : 500
Operational Rate    : 515
Accepted            : 4292
Dropped             : 0
Last Update (if any):
Punt Type           : CDP
Interface Handle    : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate         : 500
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:31:25.513.897
Platform:
  PolicerID   : 32312
  NPU: TCAM-entry    StatsID
    0:         42 0x80001cd3
    1:         42 0x80001cd3
    2:         42 0x80001cd3
    3:         42 0x80001cd3
    4:         42 0x80001cd3
    5:         42 0x80001cd3
----------------------------------------------------
----------------------------------------------------
Interface Name      : TenGigE0
Punt Reason         : MCAST
Domain              : default
Scope               : Global
State               : Active
Configured Rate     : 1000
Operational Rate    : 986
Accepted            : 0
Dropped             : 0
Last Update (if any):
Punt Type           : MCAST
Interface Handle    : 0x0800001c
Is Virtual          : 1
Is Enabled          : 1
Packet Rate         : 1000
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:32:43.210.014
Platform:
  PolicerID   : 32396
  NPU: TCAM-entry    StatsID
    0:        170 0x80001d52
    1:        172 0x80001d53
    2:        170 0x80001d52
    3:        170 0x80001d52
    4:        170 0x80001d52
    5:        170 0x80001d52
----------------------------------------------------
Interface Name      : TenGigE0
Punt Reason         : BCAST
Domain              : default
Scope               : Global
State               : Active
Configured Rate     : 1000
Operational Rate    : 986
Accepted            : 0
Dropped             : 0
Last Update (if any):
Punt Type           : BCAST
Interface Handle    : 0x0800001c
Is Virtual          : 1
Is Enabled          : 1
Packet Rate         : 1000
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:32:43.227.279
Platform:
  PolicerID   : 32397
  NPU: TCAM-entry    StatsID
    0:        171 0x80001d53
    1:        173 0x80001d54
    2:        171 0x80001d53
    3:        171 0x80001d53
    4:        171 0x80001d53
    5:        171 0x80001d53
----------------------------------------------------
```

LPTS Domain Based Policers

You can configure a particular port, a group of ports, or a line card of a router with LPTS policers of a single domain. Configuration of port-based policers that belong to a particular domain enables better categorisation and control of different types of ingress traffic. For example, since iBGP traffic has a higher rate of traffic flow, the ports that handle iBGP traffic can be configured with higher policer rates compared to the ports that handle eBGP traffic.

Restrictions

- The policer rates that are configured for ports or line cards are carried forwards as policer rates of the domain after configuring the ports or line cards as part of a domain. For example, if port hundredGigE 0/0/0/1 and port hundredGigE 0/0/0/2 have policer rate of 3000 for ospf unicast known flow and if the ports are configured as part of domain CORE, then the policer rate of domain CORE for ospf unicast known flow is 3000 unless it is configured otherwise.
- You can configure only one domain per router.
- A Domain name can be any word but can have up to a maximum of 32 characters.

Configuration Example

To configure LPTS domain based policers, use the following steps:

1. Enter the LPTS hardware configuration mode and create a domain.
2. Configure the interfaces for the domain.
3. Enter the LPTS hardware configuration mode for the domain CORE, and then configure the ingress policer rates for the domain CORE at the global level.
4. Enter the LPTS hardware configuration mode for the domain CORE, and then configure the ingress policer rates for the domain CORE at the line card level.

Configuration

```
/* Enter the LPTS hardware ingress policer configuration mode and create a domain named
CORE. */
RP/0/RP0:hostname# config
RP/0/RP0:hostname(config)# lpts pifib hardware domain CORE

/* Configure the interfaces for the domain CORE. */
RP/0/RP0:hostname(config-lpts-domains-CORE)# interface hundredGigE 0/0/0/1
RP/0/RP0:hostname(config-lpts-domains-CORE)# interface hundredGigE 0/0/0/2
RP/0/RP0:hostname(config-lpts-domains-CORE)# commit
RP/0/RP0:hostname(config-lpts-domains-CORE)# exit

/* Enter the LPTS hardware configuration mode for the domain CORE, and then configure the
ingress policer rates for the domain CORE at the global level. */
RP/0/RP0:hostname(config)# lpts pifib hardware police domain CORE
RP/0/RP0:hostname(config-lpts-policer-global-CORE)# flow ospf unicast known rate 6000
RP/0/RP0:hostname(config-lpts-policer-global-CORE)# flow ospf unicast default rate 7000
RP/0/RP0:hostname(config-lpts-policer-global-CORE)# commit
RP/0/RP0:hostname(config-lpts-policer-global-CORE)# exit
RP/0/RP0:hostname(config-lpts-policer-global)# exit
```

```
/* Enter the LPTS hardware configuration mode for the domain CORE, and then configure the
ingress policer rates for the domain CORE at the line card level. */
RP/0/RP0:hostname(config)# lpts pifib hardware police location 0/0/CPU0 domain CORE
RP/0/RP0:hostname(config-lpts-policer-global-CORE)# flow ospf unicast known rate 7000
RP/0/RP0:hostname(config-lpts-policer-global-CORE)# flow ospf unicast default rate 8000
RP/0/RP0:hostname(config-lpts-policer-global-CORE)# commit
```

Running Configuration

```
lpts pifib hardware domain CORE
 interface HundredGigE0/0/0/1
 interface HundredGigE0/0/0/2
!
lpts pifib hardware police
 domain CORE
  flow ospf unicast known rate 6000
  flow ospf unicast default rate 7000
 !

lpts pifib hardware police location 0/0/CPU0 domain CORE
 flow ospf unicast known rate 7000
 flow ospf unicast default rate 8000
 !
```

Verification

Use the following command to verify information about the LPTS domains configured:

```
RP/0/RP0:hostname# show lpts pifib domains
Thu Nov 21 15:49:31.334 IST

 Domains Information: 1 Configured
 ----------------------------------
   Domain: [1] CORE
   -----------------------
   interface [----------] HundredGigE0/0/0/1
   interface [----------] HundredGigE0/0/0/2
               0 local of total 2 interfaces
```

Defining Dynamic LPTS Flow Type

The Dynamic LPTS flow type feature enables you to configure LPTS flow types and also enables you to define the maximum LPTS entries for each flow type in the TCAM. The dynamic LPTS flow type configuration is per line card basis, hence you can have multiple profiles configured across line cards.

When the router boots, the default LPTS flow types are programmed in the TCAM. For each flow type, the maximum flow entries are predefined. Later, at runtime, you have an option to choose the flow type based on network requirements and also confirgure the maximum flow entry value. The maximum flow entry value of zero denotes that a flow type is not configured.

Note You can get the default maximum flow values for both configurable flow and non-configurable flow from the output of the following show command:

```
show lpts pifib dynamic-flows statistics location <location specification>
```

The list of configurable and non-confiurable flow types are listed in below tables. You can also use **show lpts pifib dynamic-flows statistics location** command to view the list of configurable and non-configurable flow types:

Note The sum of maximum LPTS entries that are configured for all flow types must not exceed 8000 entries per line card.

Configuration Example

In this example you will configure the BGP-known and ISIS-known LPTS flow type in the TCAM and define the maximum flow entries as 1800 and 500 for node location 0/1/CPU0 As the new maximum values are more than the default values, we have to create space in the TCAM be disabling other flow types so that the sum of maximum entries for all flow types per line card does not exceed 8000 entries. Hence RSVP-known flow type is set to zero in our example:

```
RP/0/RP0:hostname#configure
RP/0/RP0:hostname(config)#lpts pifib hardware dynamic-flows location 0/1/CPU0
RP/0/RP0:hostname(config-pifib-flows-per-node)#flow bgp known max 1800
RP/0/RP0:hostname(config-pifib-flows-per-node)#flow ISIS known max 500
RP/0/RP0:hostname(config-pifib-flows-per-node)#flow RSVP known max 0
RP/0/RP0:hostname(config-pifib-flows-per-node)#commit
```

Running Configuration

```
RP/0/RP0:hostname#
flow bgp known max 1800
flow isis known 500
flow RSVP known 0
```

Verification

This show command displays dynamic flow statistics. You can see that the flow types BGP-known and ISIS-known are configured in the TCAM with newly configured maximum flow entry value. You can also see that the RSVP-known flow type is disabled:

```
RP/0/RP0:hostname#

 Dynamic-flows Statistics:
 -------------------------
 (C - Configurable, T - TRUE, F - FALSE, * - Configured)
 Def_Max  - Default Max Limit
 Conf_Max - Configured Max Limit
 HWCnt    - Hardware Entries Count
 ActLimit - Actual Max Limit
 SWCnt    - Software Entries Count
 P, (+)   - Pending Software Entries


  FLOW-TYPE           C  Def_Max Conf_Max     HWCnt/ActLimit      SWCnt P
 -------------------- -- ------- --------   -------/--------    ------- -
 Fragment             F        2       --         2/2                 2
 OSPF-mc-known        T      600       --         2/600               2
 OSPF-mc-default      F        4       --         4/4                 4
 OSPF-uc-known        T      300       --         1/300               1
 OSPF-uc-default      F        2       --         2/2                 2
 ISIS-known           T      300       500        500/300             0
 ISIS-default         F        1       --         1/1                 1
 BGP-known            T      900      1800       1800/900             0
 BGP-cfg-peer         T      900       --         0/900               0
 BGP-default          F        4       --         4/4                 4
 PIM-mcast-default    F       40       --         0/40                0
 PIM-mcast-known      T      300       --         0/300               0
 PIM-ucast            F       40       --         2/40                2
 IGMP                 T     1200       --         0/1200              0
 ICMP-local           F        4       --         4/4                 4
 ICMP-control         F        5       --         5/5                 5
 ICMP-default         F        9       --         9/9                 9
 ICMP-app-default     F        2       --         2/2                 2
 LDP-TCP-known        T      300       --         0/300               0
 LDP-TCP-cfg-peer     T      300       --         0/300               0
 LDP-TCP-default      F       40       --         0/40                0
 LDP-UDP              T      300       --         0/300               0
 All-routers          T      300       --         0/300               0
 RSVP-default         F        4       --         1/4                 1
 RSVP-known           T      300       0          0/300               0
 SNMP                 T      300       --         0/300               0
 SSH-known            T      150       --         0/150               0
 SSH-default          F       40       --         0/40                0
 TELNET-known         T      150       --         0/150               0
 TELNET-default       F        4       --         0/4                 0
 UDP-default          F        2       --         2/2                 2
 TCP-default          F        2       --         2/2                 2
 Raw-default          F        2       --         2/2                 2
 GRE                  F        4       --         0/4                 0
 VRRP                 T      150       --         150/150             0
 DNS                  T       40       --         0/40                0
 NTP-default          F        4       --         0/4                 0
 NTP-known            T      150       --         0/150               0
 TPA                  T        5       --         0/5                 0
---------------------------
 Local Limit : 7960/8000 /*The sum of maximum flow entries configured for all flow types
                                  per line card is less than 8000*/
 HWCnt/SWCnt : 45/51
---------------------------
```

In the above show command output, the last column **P** specifies the pending software flow entries for the flow type.

APPENDIX A

System Messages

This chapter lists out the system messages that appears when you work with the OTN application.

For a release-wise listing of IOS XR System Error Messages, see https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/error/message/ios-xr-sem-guide.html

System Messages

The following error messages appear on the Permanent Connection pane.

Error Messages	Error Description
You can delete permanent connections that contains high order ODUs only.	This error message is displayed when you are deleting a connection that does not contain a high order ODUs.
Due to an error on the node, the XML query failed.	This error message is displayed when you are deleting a node.
You cannot delete multiple rows simultaneously	This error message is displayed when you are trying to delete multiple rows at one time.
XConnect ID is a mandatory field. Enter a value before proceeding.	This error message is displayed when you have not entered a value in the XConnect ID.
Select the End Point 1 value from the drop-down list.	This error message is displayed when you have not selected any value for End Point 1 from the drop-down list.
Select the End Point 2 value from the drop-down list.	This error message is displayed when you have not selected any value for End Point 2 from the drop-down list.
Enter the valid range of XConnect ID from 1 to 32655.	This error message is displayed when the value entered for XConnect ID is not within the specified range.
The XConnect ID that you entered already exists. Enter a unique XConnect ID.	This error message is displayed when you have entered a XConnect ID that already exists in the database.
Select the correct End Point 1, End Point 2 value.	This error message is displayed when the value entered for End Point 1 and 2 does not match the standard specified.

Error Messages	Error Description
The End Point 1 interface that you selected is already cross connected. Select another End Point 1 interface.	This error message is displayed when the selected End Point 1 interface is already a cross connect.
The End Point 2 interface that you selected is already cross connected. Select another End Point 2 interface.	This error message is displayed when the selected End Point 2 interface is already a cross connect.

The following error messages appear on the Explicit Path pane.

Error Messages	Error Description
Explicit path name be unique.	This error message is displayed when the value entered for the Explicit Path Name already exists in the database.
You cannot delete multiple rows simultaneously.	This error message is displayed when you are deleting multiple rows at one time.
Due to an error on the node, the XML query failed.	This error message is displayed when you are deleting a node.

The following error messages appear on the CcdOTNAttrs Pane.

Error Messages	Error Description
The circuit name must not exceed 64 characters.	This error message is displayed when the circuit name that you have entered has exceeded the specified limit (64 characters).
Source Node is a mandatory field. Select the source node from the drop-down list before proceeding.	This error message is displayed when you have not selected any options from the Source Node drop-down list.
Enter Unique values in Source and destination node.	This error message is displayed when you have entered either the same name for both Source and Destination or the name already exits in the database.
Destination Node is a mandatory field. Select the destination node from the drop-down list before proceeding.	This error message is displayed when you have not selected any options from the destination drop-down list.
Source Client Interface is a mandatory field. Select the value from the drop-down list.	This error message is displayed when you not selected any value for Source Client Interface from the drop-down list.
Destination Client Interface is a mandatory field. Enter a value before proceeding.	This error message is displayed when you have not selected Destination Client Interface from the drop-down list.
Working Path Option is a mandatory field. Configure before proceeding.	This message is displayed when you have not configured a Working Path Option.
Bandwidth configuration for ODUFlex is a mandatory field. Configure before proceeding.	This error message is displayed when you have not configured a bandwidth for ODUFLex.

The following error messages appear on the OTNPathOptionDlg Pane.

Error Messages	Error Description
Path Option Index is a mandatory field. Enter a value before proceeding.	This error message is displayed when the entered value in Path Option Index is not blank or not valid.
The Bit rate range must be from 1-104857600	This error message is displayed when the bit rate range is not within the specified limit.
In a single circuit, multiple working paths are not supported.	This error message is displayed when you have entered multiple paths in single circuit.
Enter a unique Path Option ID.	This error message is displayed when you have entered a path that already exits in the database.
Select an explicit path to proceed.	This error message is displayed when you have entered a path that is not explicit.

The following error messages appear on the SppGeneralPane.

Error Messages	Error Description
Are you sure you want to delete the selected NTP/SNTP instance?	This message is displayed on the Chassis View > Provisioning > Rest of SPP General > SppGeneralPane when you want to delete a selected NTP/SNTP.
The NTP/SNTP instance that you want to delete is either missing or has failed.	This error message is displayed on the Chassis View > Provisioning > Rest of SPP General > SppGeneralPane when you are deleting an NTP/SNTP instance that is missing.
A significant change in time might not validate the node performance monitoring counter. Do you still wish to continue?	This message is displayed on the Chassis View > Provisioning > Rest of SPP General > SppGeneralPane when you have entered a changed time due to which node performance monitoring counter cannot be validated.
Name is a mandatory field. Enter a value before proceeding.	This error message is displayed on the Chassis View > Provisioning > Rest of SPP General > SppGeneralPane when you have not entered a already existing name.
TL1 name should not exceed 20 characters. This node will not be visible to the GNE for TL1 access.	This error message is displayed on the Chassis View > Provisioning > Rest of SPP General > SppGeneralPane when the name limit has exceeded the specified limit for TL1.
Do you wish to continue?	This error message is displayed on the Chassis View > Provisioning > Rest of SPP General > SppGeneralPane when you have made any changes.
The Node Name/TID (newNodeName)is invalid, must not contain spaces. You will be unable to open a TL1 session to this node, by using the (newNodeName) node name or TID.	This error message is displayed on the Chassis View > Provisioning > Rest of SPP General > SppGeneralPane when there is a space in the node name or TID.

The following error messages appear on the SmpDBPane.

Error Messages	Error Description
The abc.txt file already exists. Do you want to replace it?	This error message is displayed on the Maintenance > Audit, Backup n Restore > SmbDBPane when you are saving a file with the name that is already there in the database.
Archive audit trail is complete.	This message is displayed on the Maintenance > Audit, Backup n Restore > SmbDBPane when archive audit trail is completed.
Select a file to save the backup.	This message is displayed on the Maintenance > Audit, Backup n Restore > SmbDBPane when you have not selected a file to save the backup.
Backup of database is complete.	This message is displayed on the Maintenance > Audit, Backup n Restore > SmbDBPane when the backup of the database is complete.
Select a file from which you want to restore the database.	This message is displayed on the Maintenance > Audit, Backup n Restore > SmbDBPane when the backup of the database is complete.
Restoring database from another node or an earlier backup might result in loss of traffic. Do you still wish to continue?	This message is displayed on the Maintenance > Audit, Backup n Restore > SmbDBPane when you are restoring the database from another node or an earlier backup as it may result in loss of traffic.

The following error messages appear on the PM thresholds.

Error Messages	Error Description
Do you really want to reset the threshold values to their default values?	This error message is displayed on the Card > Provisioning > PM Thresholds > Optics when you want to reset the threshold values to its default value.
Select a controller to reset its threshold values.	This error message is displayed on the Card > Provisioning > PM Thresholds when you have not selected a controller to reset the threshold value.
Do you really want to reset the threshold values to their default values?	This error message is displayed on the Card > Provisioning > PM Thresholds > TCM when you want to reset the threshold values to its default value.
Select a TCM to reset the default threshold value.	This error message is displayed on the Card > Provisioning > PM Thresholds > TCM when you have not selected a TCM to reset the threshold value.

The following error messages appear on the Performance tab.

Error Messages	Error Description
The statistics for the selected controller on the given card will be permanently cleared. Do you really want to initialize all registers in the selected column to zero?	This error message is displayed on the Card > Performance > Optics when on a given card you are clearing the statistics for the selected controller, that will initialize all the registers to zero.

Error Messages	Error Description
Select the controller column to clear its statistics values.	This error message is displayed on the Card > Performance > FEC when you have not selected the controller column to clear the controller's statistics values.

The following error messages appear on the PM thresholds.

Error Messages	Error Description
Do you really want to reset the threshold values to their default values?	This error message is displayed on the Circuit > Edit Dialog > ODU Configuration > PM Thresholds > ODU > when you want to reset the threshold values to its default value.
Do you really want to reset the threshold values to their default values?	This error message is displayed on the Circuit > Edit Dialog > ODU Configuration > PM Thresholds > TCM > when you want to reset the threshold values to its default value.

The following error messages appear on the Performance.

Error Messages	Error Description
The statistics for the selected controller on the given card will be permanently cleared. Do you really want to initialize all registers in the selected column to zero?	This error message is displayed on the Circuit > Edit Dialog > Performance > ODU pane when on a given card you are trying to clear the statistics for the selected controller, that initializes all registers to zero.
Select a controller(column) to clear respective statistics values.	This error message is displayed on the Node view > Maintenance > Software pane when you have not selected a controller to reset its threshold value.
Last Install Log Text field is a mandatory field. Enter a value before proceeding.	This error message is displayed on the Node view > Maintenance > Software pane when the Last Install Log Text field is empty.
Package is already added.	This error message is displayed on the Node view > Maintenance > Software pane when you are deleting to add an existing package.
Special characters are not supported in a file path.	This error message is displayed on the Node view > Maintenance > Software pane when you enter a special character in a file path.
The prefix in a file path must be 'tftp://server/directory/', 'harddisk:/directory/', 'sftp://user@server:/directory/', "'ftp://user@server:/directory/' or '/dir/'.	This error message is displayed on the Node view > Maintenance > Software pane when the prefix in the file path is not 'tftp://server/directory/', 'harddisk:/directory/', 'sftp://user@server:/directory/', "'ftp://user@server:/directory/' or '/dir/'.
Path File Name is a mandatory field. Enter a value before proceeding.	This error message is displayed on the Node view > Maintenance > Software pane when the path name entered is not valid.

The following error messages appear on the ODUTTI Pane.

Error Messages	Error Description
This is a destination node controller. Select another controller.	This error message is displayed on the ODUTTI pane when you have selected a destination node controller.
Transmit Operator String for controller is a mandatory filed. Enter a value before proceeding	This error message is displayed on the ODUTTI pane when you want to configure the Transmit Operator String for controller.
Expected Operator String for controller is a mandatory filed. Enter a value before proceeding.	This error message is displayed on the ODUTTI pane when you want to configure the Expected Operator String for controller.
In an hexadecimal string, the character count must be even.	This error message is displayed on the ODUTTI pane when the character count is not even.

The following error messages appear on the TCMEdit Pane.

Error Messages	Error Description
Transmit Operator String for controller is a mandatory filed. Enter a value before proceeding.	This error message is displayed on the TCMEdit pane when you want to configure the Transmit Operator String for controller.
Expected Operator String for controller is a mandatory filed. Enter a value before proceeding.	This error message is displayed on the TCMEdit pane when you want to configure the Expected Operator String for controller.
TCM controller is a mandatory filed. From the drop-down list, select a value for the controller R/S/I/P.	This error message is displayed on the TCMEdit pane when you have not selected or selected a wrong TCM to be configured for the controller.
Select a different node to configure the controller.	This error message is displayed on the TCMEdit pane when you have selected a wrong node to configure the controller.
In an hexadecimal string, the character count must be even.	This error message is displayed on the TCMEdit pane when the character count is not even.

The following error messages appear on the OSPF and OSPF-TE Pane.

Error Messages	Error Description
Due to an error on the node, the XML query failed.	This error message is displayed on the OSPF and OSPF-TE pane when the area of configuration is not stored.

The following error messages appear on the Controllers.

Error Messages	Error Description
The admin state is not configured as OOS,DSBLD.	This error message is displayed on the Card View > Provisioning > Controllers > OTU window when the admin state is not configured as OOS,DSBLD.
Do you wish to apply the changes?	This error message is displayed on the Card View > Provisioning > Controllers > Section Trace window when you have made some changes and want the changes to be applied.

Error Messages	Error Description
The value in the Transmitted field is too long. Is it okay to truncate it to the new string?	This error message is displayed on the Card View > Provisioning > Controllers > Section Trace window when in the Transmitted field the value is too long and it is suppose get truncated to the new string.
Setting the Trace fields to their factory defaults might cause traffic loss. Do you still wish to continue?	This error message is displayed on the Card View > Provisioning > Controllers > Section Trace window when you are about the set the Trace fields to default

The following error messages appear on the Network OTU (SRLGs) sub tab.

Error Message	Error Description
Enter a value from 0 to 4294967294.	This error message is displayed on the Card View > Provisioning > Network SRLG > OTU (SRLGs) when the value is not within the range (specified).
Enter the value from 1 to 17	This error message is displayed on the Card View > Provisioning > Network SRLG > OTU (SRLGs) when the value is not within the range (specified).
SRLG is a mandatory field. Enter a value before proceeding.	This error message is displayed on the Card View > Provisioning > Network SRLG > OTU (SRLGs) when SRLG ID is not unique.

The following error messages appear on the Port Modules sub tab.

Error Messages	Error Description
PortMode is a mandatory field. Enter a value before proceeding.	This error message is displayed on the Card View > Provisioning > Port Module to enter the value in PortMode.
The capacity of 24xOC48 card has exceeded.	This error message is displayed on the Card View > Provisioning > Port Module when 24xOC48 card exceeds its capacity.
The port does not support the framing type that you have selected.	This error message is displayed on the Card View > Provisioning > Port Module when you have not selected the correct framing type.
Select the value as None, from the drop-down list.	This error message is displayed when the value is not selected as None.

The following error messages appear on the Maintenance tab.

Error Messages	Error Description
This configuration is not supported because a loopback is configured.	This messages is displayed on the Card View > Maintenance > Loopback window, when your configuration is not supported as loopback is not configured.
Change the admin state to OOS,MT.	This warning is displayed on the Card View > Maintenance > Loopback window to change the admin state to OOS,MT.

APPENDIX B

Administrative and Service States

This chapter gives description of different administrative and service states.

Administrative and Service States

Administrative State	Definition
IS	Puts the entity in service.
OOS,DSBLD	Removes the entity from service and disables it.
OOS,MT	Removes the entity from service for maintenance.

Service State	Definition
OOS-MA,DSBLD	The entity was manually removed from service and does not provide its provisioned functions. All the services are disrupted and unable to carry traffic.
OOS-MA,MT	The entity has been manually removed from service for a maintenance activity but still performs its provisioned functions.
OOS-AUMA,FLT&MT	The entity is not operational because of an autonomous event and has also been manually removed from service for a maintenance activity.
OOS-MA,LPBK&MT	The entity has been manually removed from service for a maintenance activity but still performs its provisioned functions. A loopback is present on the resource.
OOS-AUMA, FLT & LPBK & amp; MT	The entity is unlocked with loopback configured. However, the service is not operational due to some failure. All the defects are raised and cleared but the end user is not notified.
OOS-AU,AINS	The entity is not operational because of an autonomous event. The entity is delayed before moving to the IS-NR state.
OOS-AU,AINS&FLT	The entity is unlocked. However, the service is not operational due to some failure. All the defects are raised and cleared but the end user is not notified. When all the defects are cleared and the resource returns operational, the AINS window is restarted.

Service State	Definition
IS-NR	The entity is fully operational and will perform as provisioned.
OOS-AU,FLT	The entity is unlocked and not operational due to a failure. This happens when the secondary state is normal and there are defects.