Configuration Guide for Cisco NCS 1002, IOS XR Release 6.3.x

First Published: 2017-08-01

Last Modified: 2019-03-04

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

New and Changed Information vii

CHAPTER 1

Configuring Slices 1

Understanding Cisco NCS 1002 1

Slice and Port Numbering 2

Supported Configurations 2

Configure the Slice 3

Verify Slice Configuration 5

Illustrations for Supported Configurations 8

CHAPTER 2

Configuring Controllers 11

Optics Controllers 11

Maintenance Mode 12

Configure Optics Controller 12

Configure Wavelength 13

Breakout Mode 13

Laser Squelching 14

LLDP Snooping 14

LLDP Snoop and Drop 16

Configuring Slices and LLDP Drop at Slice Level 16

Verifying the Status of LLDP Drop 17

Disabling LLDP Drop 19

Configure Ethernet Controller 19

Configure the Coherent DSP Controller 20

Configure Loopback 20

Restore Factory Settings 21

Headless Mode 21
View the Headless Statistics 21

CHAPTER 3 Configuring IP Access List 23
Configure IP Accesss List 23
Verify IPv6 ACL 24

CHAPTER 4 Configuring Performance Monitoring 25
Configure PM Parameters 25
View PM Parameters 27
Pseudo Random Binary Sequence 31
Configuring Pseudo Random Binary Sequence 31
Viewing PRBS Performance Monitoring Parameters 32
Verifying PRBS 32

CHAPTER 5 Configuring MACsec Encryption 35
MACsec Frame Format 36
MACsec SECTag Format 37
MACsec Key Agreement 37
MACsec in NCS 1002 37
Supported Configurations in Encrypted Mode 38
Illustrations for Supported Configurations in Encrypted Mode 39
Configure MACsec Encryption Using PSK Authenication 40
MACsec Key Chain 40
Configure MACsec Key Chain 41
Verify MACsec Key Chain 42
MACsec Policy 43
Configure MACsec Policy 43
Verify MACsec Policy 45
MACsec Controllers 46
Configure the Slice 46
Verify Slice Configuration 48
Apply MACsec Configuration on MACsec Controller 51
Verify MACsec Configuration on MACsec Controller 52

Verify State of MACSec Controller 56
SecY Statistics 56
Trunk Side Statistics 59
Control Plane Statistics 60
Configuring MACsec Threshold Crossing Alerts 61
View MACsec PM Parameters 62
MACsec MKA Using EAP-TLS Authentication 68
IEEE 802.1X Device Roles 68
Prerequisites for MACsec MKA Using EAP-TLS Authentication 68
Configure MACsec Encryption Using EAP-TLS Authentication 69
Configure RADIUS Server 69
Configure 802.1X Authentication Method 70
Generate RSA Key Pair 71
Configure Trust Point 71
Authenticate Certificate Authority and Request Certificates 72
Configure EAP Profile 73
Configure 802.1X Profile 74
Configure EAP and 802.1X Profile on MACsec Controller 75
Verify EAP and 802.1X Configuration on MACsec Controller 76

CHAPTER 6 **Configuring GMPLS UNI 79**
Configuring GMPLS UNI 81
Configure LMP and Alien Wavelength in NCS 2000 Series Node 82
Configure Unnumbered LMP in NCS 2000 Series Node 83
Retrieve Ifindex from NCS 2000 Series Node 83
Configure LMP in Cisco NCS 1002 84
Configure RSVP in NCS 1002 84
Configure MPLS Tunnel in NCS 1002 85
Headless Mode and GMPLS UNI 85
Display GMPLS UNI Tunnel, RSVP, and LMP Information 85
Example of MPLS Tunnel Creation Without ERO 90
Example of MPLS Tunnel Creation with ERO 91
Example of MPLS Tunnel Creation with XRO 92
Example of MPLS Tunnel Creation with Explicit Signaled Wavelength 93

Validate GMPLS Assigned Channel Number (6.25 Ghz) over Coherent DSP 93

CHAPTER 7 **Configuring Breakout Patch Panel 97**

Breakout Patch Panel 97

Configure Breakout Patch Panel 97

CHAPTER 8 **Smart Licensing 101**

Understanding Smart Licensing 101

Benefits of Smart Licensing 104

PIDs of NCS 1002 104

Software Entitlements and Smart Licenses of Cisco NCS 1002 105

Creating a Token 106

Configuring Smart Licensing 106

Verifying Smart Licensing Configuration 107

APPENDIX A **Configuring SNMP 111**

New and Changed Information

See the Workflow document to refer the other guides of NCS 1002.

This table summarizes new and changed information for configuration guide for Release 6.3.2, and lists where the features are documented.

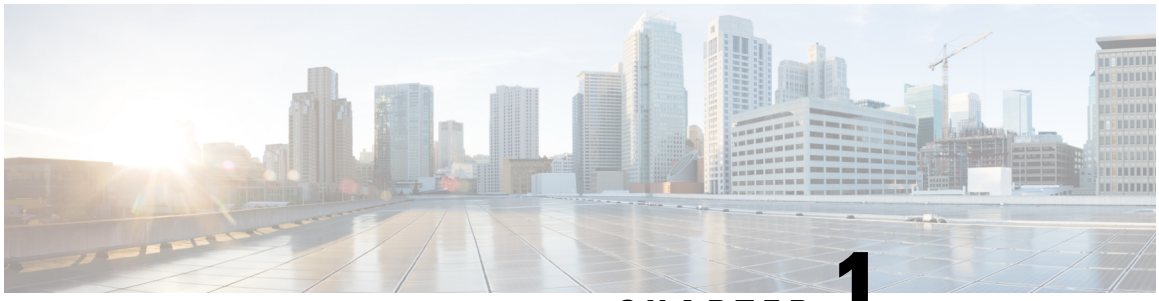
Table 1: New and Changed Features - R6.3.2

Feature	Description	Where Documented
GMPLS UNI Flexible Grid	The user can create a GMPLS optical channel trail (OCH Trail) in a network where the NCS 1002 node is connected to a NCS 2000 series node. GMPLS UNI flexible grid is supported from R6.3.2 that supports 250G channels and 6.25 GHz channel spacing.	Configuring GMPLS UNI, on page 79
IPv6 ACL	NCS 1002 supports the following IP Acces List (ACL): • Ingress ACL for both IPv4 and IPv6. • Egress ACL: Self-Originated Packet is not supported by ACL, as this is already controlled by user. Only forwarded packets or traffic is classified under ACL. This rule is applicable for both IPv4 and IPv6 ACL.	Configure IP Accesss List, on page 23
MACsec SNMP	The following MIB is supported in NCS 1002. IEEE8021-SECY-MIB (only SNMP read-only operations are supported for this MIB).	Configuring SNMP, on page 111

Feature	Description	Where Documented
MACsec Threshold Crossing Alerts	The user can configure MACsec Threshold Crossing Alerts (TCA) at mac-sec ether, secy-if (interface), secy-tx,and secy-tx. There is no default threshold, minimum, or maximum threshold to configure MACsec TCA. The user must enable MACsec controllers to view MACsec performance. To configure MACsec threshold crossing alerts and the performance monitoring parameters, see the Configuring MACsec Encryption chapter in the Configuration Guide for Cisco NCS 1002.	Configuring MACsec Threshold Crossing Alerts, on page 61
MACsec MKA Using EAP-TLS Authentication	Using IEEE 802.1X port-based authentication with Extensible Authentication Protocol (EAP-TLS), MACsec MKA can be configured between two NCS 1002 device ports. EAP-TLS allows mutual authentication and obtains MSK (master session key or primary session key). Both Connectivity Association Key Name (CKN) and connectivity association key (CAK) are derived from MSK for MKA operations. The device certificates are carried for authentication to the external AAA server using EAP-TLS.	MACsec MKA Using EAP-TLS Authentication , on page 68
Mixed Mode Configuration	The first three client ports of a slice can be configured at 100G bitrate and the last two client ports can be configured at 10G bitrate per lane. This feature is called mixed mode configuration.	Configuring Slices, on page 1

Feature	Description	Where Documented
PRBS	Pseudo Random Binary Sequence (PRBS) feature allows the user to perform data integrity checks between the trunk links of NCS 1002 without enabling the client traffic. PRBS generator generates a bit pattern on the device and sends it to the peer device, where PRBS analyzer detects if the transmitted bit pattern is preserved. The user can configure the trunk port in one of the following modes for PRBS. • Source Mode • Sink Mode • Source-Sink Mode	Pseudo Random Binary Sequence, on page 31

New and Changed Information



CHAPTER 1

Configuring Slices

This chapter describes the procedures to configure slices and supported configurations on the client and trunk ports of each slice.

- Understanding Cisco NCS 1002 , on page 1
- Slice and Port Numbering, on page 2
- Supported Configurations, on page 2
- Configure the Slice, on page 3
- Verify Slice Configuration, on page 5
- Illustrations for Supported Configurations, on page 8

Understanding Cisco NCS 1002

Cisco NCS 1002 is a 2Tbps muxponder that addresses the growing bandwidth needs of data center DWDM applications. The muxponder is 2 RU. It provides dense, low power, and cost-optimized DWDM transport for 10G, 40G, and 100G clients. The trunk ports can operate at 100G, 200G, and 250G traffic. NCS 1002 is ROHS6 compliant.

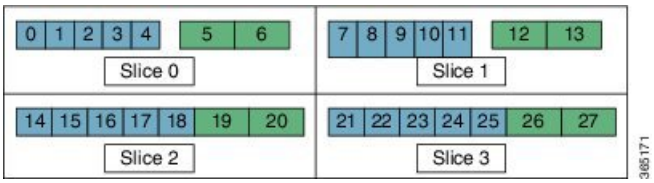
NCS 1002 has four independent slices. A slice is a group of client and trunk ports operating homogeneously. Each slice contains five QSFP+/QFSP28 client optical ports and two CFP2 DWDM trunk ports. Each slice delivers up to 500 Gbps traffic. NCS 1002 has one controller card, two Solid State Disks (SSD), 1+1 redundant 1800W AC power supply modules, and 2+1 redundant fans.

NCS 1002 delivers the following benefits:

- Supports up to 2 Tbps capacity
- Transports 100, 200, or 250Gbps per wavelength on the same platform through software provisioning
- Transports 10 GE, 40 GE, and 100 GE on the same platform through software provisioning
- Supports grid-less tuning for flex-grid dense wavelength-division multiplexing (DWDM)
- Supports different modulation formats (PM-QPSK or PM-16QAM)
- Supports 7% or 20% Soft Decision (SD) FEC for maximum optical performance
- Allows for automated installation, configuration and monitoring
- Supports machine-to-machine (M2M) APIs based on YANG models for ease of configuration
- Supports a telemetry agent for a pub-sub model of device monitoring

Slice and Port Numbering

Figure 1: Slice and Port Numbering



The slices are numbered from 0 to 3. The ports are numbered across the different slices from 0 to 27. The port numbers against blue background represent client ports; port numbers against green background represent trunk ports.

Supported Configurations

The following configurations are supported on client and trunk ports in each slice. Each slice contains up to twenty Ethernet client ports operating at 10G, or five Ethernet client ports operating at 100G, or five Ethernet client ports operating at 40G. The client ports map to two trunk ports operating at 100G, 200G, or 250G that provides muxponder functionality.

In mixed mode configuration, each slice contains up to three Ethernet client ports operating at 100G and eight Ethernet client ports operating at 10G. The client ports map to two trunk ports operating at 200G.

40G client ports are supported from R6.0.1.

Client Ports	Trunk Ports
20 x 10G	2 x 100G
20 x 10G	1 x 200G
4 x 40G	2 x 100G
5 x 40G	1 x 200G
2 x 100G	2 x 100G
4 x 100G	2 x 200G
5 x 100G	2 x 250G
3 x 100G + 8 x 10G	2 x 200G

All configurations can be accomplished using appropriate values for client bitrate and trunk bitrate parameters of the **hw-module** command.

Configure the Slice

You can configure the slice with traffic on client and trunk ports. All five client ports of the slice need to be configured at the same bitrate except for mixed mode configuration. Both the trunk ports are always set with the same FEC mode. The slice can be configured to send encrypted traffic from R6.1.1.

See the Supported Configurations in Encrypted Mode, on page 38 section to determine the supported configurations on the client and trunk ports in each slice configured in encrypted mode

Note When the slice is configured in encrypted mode, the drop-lldp cannot be enabled.

Note When NCS 1002 is installed in a system where both the trunk interfaces in a slice are used, the two 250Gb 16QAM signals need to be co-routed on the same fiber (mandatory when the 5x100Gb client port is provisioned). Also, it is recommended to use adjacent wavelengths when the line modulation is set to 250Gb 16QAM. The reason for this is that the chromatic dispersion generates skew between wavelengths. Assuming a Dispersion of 10000 ps/nm, a span of 500 km, and using adjacent channel, the skew is evaluated in less than 200 ns and it is compensated by the deskew capability of NCS 1002. If the delta between the used channels is increased, the skew increases and it might exceed the skew compensation done by NCS 1002.

To configure the slice with unencrypted traffic, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate** { **10G** | **40G** | **100G** } **trunk bitrate** { **100G** | **200G** | **250G** } **fec** { **softdecision7** | **softdecision20** }

commit

To configure the slice with mixed mode, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate 10G-100G trunk bitrate 200G fec** { **softdecision7** | **softdecision20** }

commit

To configure the slice with encrypted traffic, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate** { **10G** | **40G** | **100G** } **trunk bitrate** { **100G** | **200G** } **fec** { **softdecision7** | **softdecision20** } [**encrypted**]

commit

Examples

The following is a sample in which slice 0 is configured in mixed mode, and FEC on the trunk ports is set to softdecision7.

```
configure
```

```
hw-module location 0/RP0/CPU0 slice 0 client bitrate 10G-100G trunk bitrate 200G fec
SoftDecision7
commit
```

The following is a sample in which slice 0 is configured to send encrypted traffic with 100G client rate, 200G trunk rate, and FEC on the trunk ports is set to softdecision7.

```
configure
hw-module location 0/RP0/CPU0 slice 0 client bitrate 100G trunk bitrate 200G softdecision7
 encrypted
commit
```

The following is a sample in which slice 0 is configured to send encrypted traffic with 10G client rate, 100G trunk rate, and FEC on the trunk ports is set to softdecision20. When a slice is configured with 10G client rate in encrypted mode, ten MACsec controllers are created for each slice. When all the four slices are configured with 10G client rate in encrypted mode, forty MACsec controllers are created for NCS 1002. Two MACsec controllers are created for the middle port, four controllers for the fourth port, and four controllers for the fifth port per slice.

```
configure
hw-module location 0/RP0/CPU0 slice 0 client bitrate 10G trunk bitrate 100G softdecision20
 encrypted
commit
```

The following is a sample in which slice 0 is configured to send encrypted traffic with 40G client rate, 100G trunk rate, and FEC on the trunk ports is set to softdecision20.

```
configure
hw-module location 0/RP0/CPU0 slice 0 client bitrate 40G trunk bitrate 100G softdecision20
 encrypted
commit
```

The following is a sample to configure all the slices with a specific client rate and trunk rate.

```
configure
hw-module location 0/RP0/CPU0 slice all client bitrate 10G trunk bitrate 100G fec
softDecision7
commit
```

```
configure
hw-module location 0/RP0/CPU0 slice all client bitrate 40G trunk bitrate 100G fec
softDecision7
commit
```

```
configure
hw-module location 0/RP0/CPU0 slice all client bitrate 100G trunk bitrate 200G fec
softDecision7
commit
```

The following is a sample to remove the configuration from all the slices.

```
configure
no hw-module location 0/RP0/CPU0 slice all client bitrate 10G trunk bitrate 100G fec
softDecision7
commit
```

```
configure
no hw-module location 0/RP0/CPU0 slice all client bitrate 40G trunk bitrate 100G fec
```

```
softDecision7
commit
```

```
configure
no hw-module location 0/RP0/CPU0 slice all client bitrate 100G trunk bitrate 200G fec
softDecision7
commit
```

Associated Commands

- hw-module
- show hw-module

Verify Slice Configuration

Use this procedure to verify whether the slice is correctly configured.

show hw-module { **slice** [*slicenumber* | **all**] }

Example:

```
RP/0/RP0/CPU0:ios# show hw-module slice 0


Thu Aug 11 16:16:58.935 IST
Slice ID:                0
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
LLDP Drop Enabled:       FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/6
Traffic Split Percentage

HundredGigECtrlr0/0/0/3                  100
HundredGigECtrlr0/0/0/4                  100
```

```
RP/0/RP0/CPU0:ios# show hw-module slice 0


Sun Dec 18 13:59:18.805 IST
Slice ID:                0
Status:                  Provisioned
Client Bitrate:          40
Trunk Bitrate:           100
DP FPGA FW Type:         MM40
DP FPGA FW Version:      03.00
HW Status:               CURRENT

Encryption Supported:    TRUE
LLDP Drop Enabled:       FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/6
Traffic Split Percentage

FortyGigECtrlr0/0/0/3                    100
```

```
FortyGigECtrlr0/0/0/4                    100

RP/0/RP0/CPU0:ios# show hw-module slice 1

Tue Jan  1 06:55:12.293 UTC
Slice ID:                1
Status:                  Provisioned
Client Bitrate:          10
Trunk Bitrate:           100
DP FPGA FW Type:         MM10
DP FPGA FW Version:      03.00
HW Status:               CURRENT

Encryption Supported:    TRUE
LLDP Drop Enabled:       FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/13
Traffic Split Percentage

TenGigECtrlr0/0/0/9/1                           100
TenGigECtrlr0/0/0/9/2                           100
TenGigECtrlr0/0/0/10/1                          100
TenGigECtrlr0/0/0/10/2                          100
TenGigECtrlr0/0/0/10/3                          100
TenGigECtrlr0/0/0/10/4                          100
TenGigECtrlr0/0/0/11/1                          100
TenGigECtrlr0/0/0/11/2                          100
TenGigECtrlr0/0/0/11/3                          100
TenGigECtrlr0/0/0/11/4                          100
RP/0/RP0/CPU0:ios# show hw-module slice 2

Slice ID:                2
Status:                  Provisioned
Client Bitrate:          10,100
Trunk Bitrate:           200
DP FPGA FW Type:         RMM
DP FPGA FW Version:      04.00
HW Status:               CURRENT

Encryption Supported:    FALSE
LLDP Drop Enabled:       FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/19  CoherentDSP0/0/0/20
Traffic Split Percentage

HundredGigECtrlr0/0/0/14                        100                   0
HundredGigECtrlr0/0/0/15                        100                   0
HundredGigECtrlr0/0/0/16                          0                 100
TenGigECtrlr0/0/0/17/1                            0                 100
TenGigECtrlr0/0/0/17/2                            0                 100
TenGigECtrlr0/0/0/17/3                            0                 100
TenGigECtrlr0/0/0/17/4                            0                 100
TenGigECtrlr0/0/0/18/1                            0                 100
TenGigECtrlr0/0/0/18/2                            0                 100
TenGigECtrlr0/0/0/18/3                            0                 100
TenGigECtrlr0/0/0/18/4                            0                 100
```

Displays the details of the slice such as the slice ID, client rate, trunk rate, and the traffic percentage carried on the trunk ports. The **Encryption Supported** field indicates whether the slice is provisioned with firmware that supports encryption or not.

Note The HW Status field might display "Need Upgrade" when the user needs to use the MACsec feature and upgrades from R6.0.1 to 6.1.1. Hence, the control FPGA (CTRL_BKP_UP, CTRL_BKP_LOW, CTRL_FPGA_UP, and CTRL_FPGA_LOW) needs to be upgraded to the latest firmware version provided by R6.1.1. See Verify Firmware Version for more information.

The Provisioned status does not indicate that the traffic can flow immediately. For example, use the **show controllers maCSecCtrlr 0/0/0/3** command output to view the provisioning information of the port after the slice is provisioned.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module slice all


Thu Aug 11 16:16:58.935 IST
Slice ID:                0
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/6
Traffic Split Percentage

HundredGigECtrlr0/0/0/3                   100
HundredGigECtrlr0/0/0/4                   100

Slice ID:                1
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/13
Traffic Split Percentage

HundredGigECtrlr0/0/0/10                   100
HundredGigECtrlr0/0/0/11                   100

Slice ID:                2
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/20
Traffic Split Percentage

HundredGigECtrlr0/0/0/17                   100
HundredGigECtrlr0/0/0/18                   100

Slice ID:                3
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
```

```
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/27
Traffic Split Percentage

HundredGigECtrlr0/0/0/24                  100
HundredGigECtrlr0/0/0/25                  100
```

Associated Commands

- hw-module
- show hw-module

Illustrations for Supported Configurations

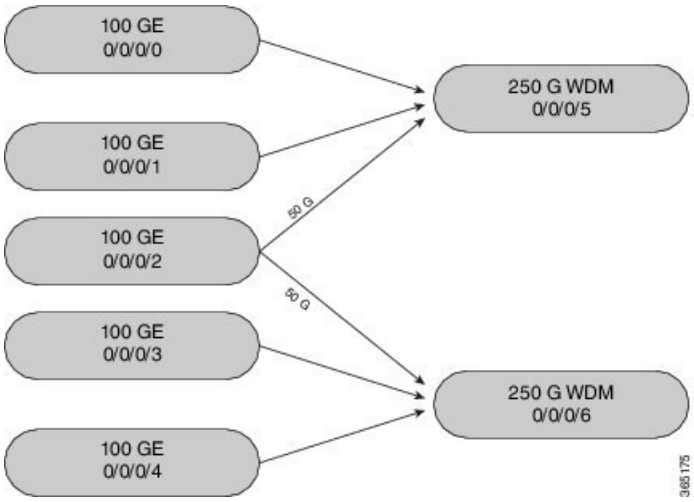
The following table describes the client and trunk ports in slice 0 that are enabled or disabled for each supported configuration.

Client Data Rate	Trunk Data Rate	Client Port 0	Client Port 1	Client Port 2	Client Port 3	Client Port 4	Trunk Port 5	Trunk Port 6
100G	100G	E	D	D	D	E	E	E
100G	200G	E	E	D	E	E	E	E
100G	250G	E	E	E	E	E	E	E
10G	100G	E	E	E	E	E	E	E
10G	200G	E	E	E	E	E	D	E
40G	100G	E	E	D	E	E	E	E
40G	200G	E	E	E	E	E	D	E

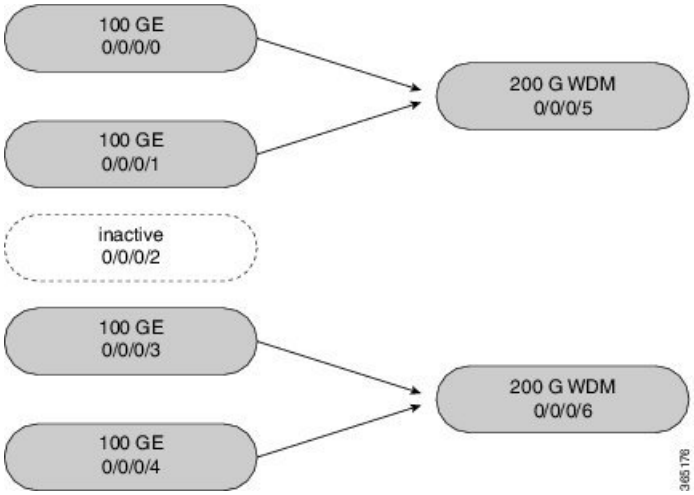
E indicates that the port is enabled; D indicates that the port is disabled.

The following illustrations describe the mapping of traffic from client to trunk ports for certain configurations.

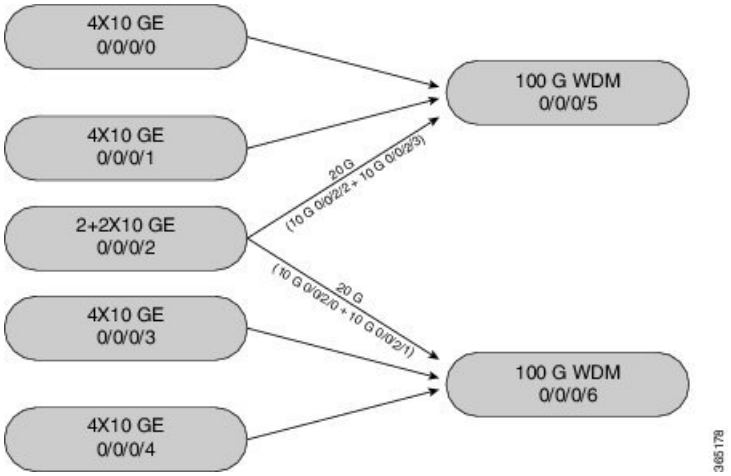
Client: 5 x 100G Trunk: 2 x 250G



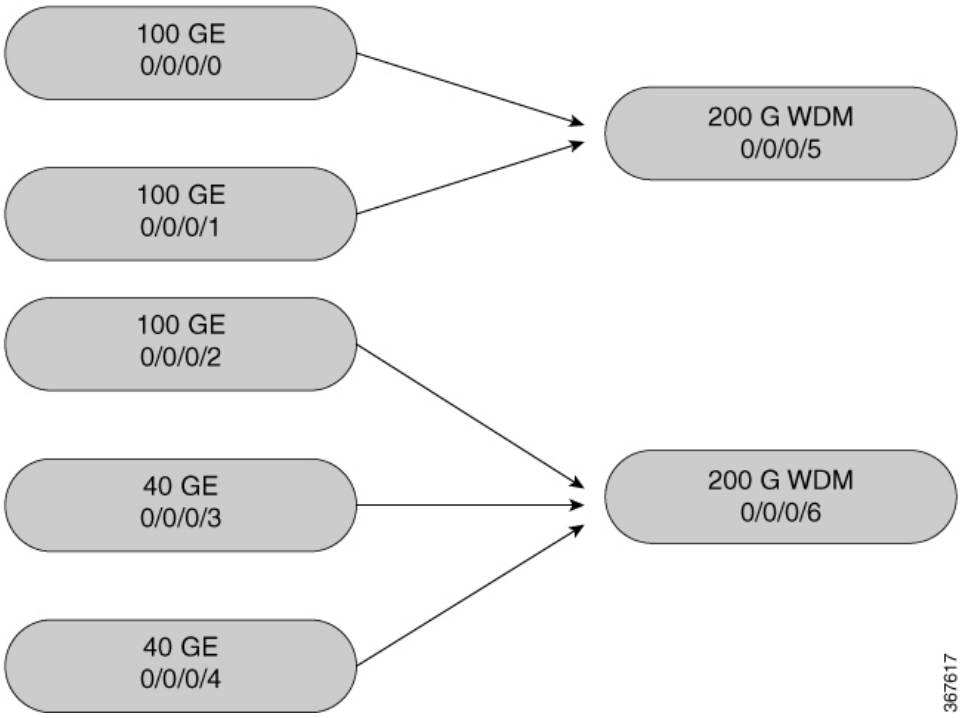
Client: 4 x 100G Trunk: 2 x 200G

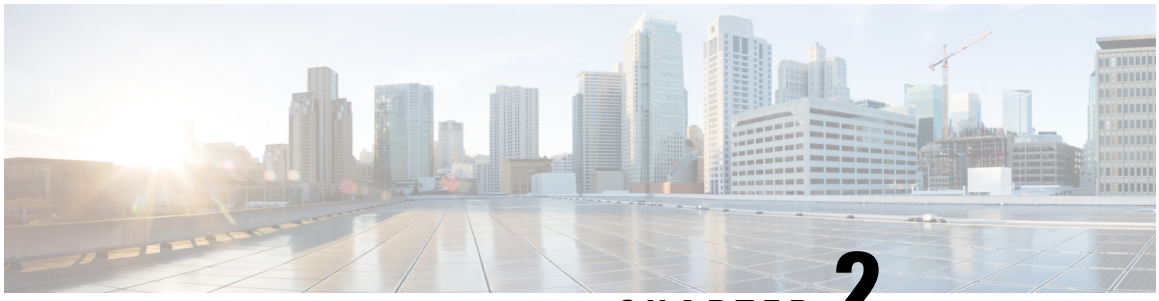


Client: 20 x 10G Trunk: 2 x 100G



The following illustration describes the mapping of traffic from client to trunk ports for mixed mode configuration.





CHAPTER 2

Configuring Controllers

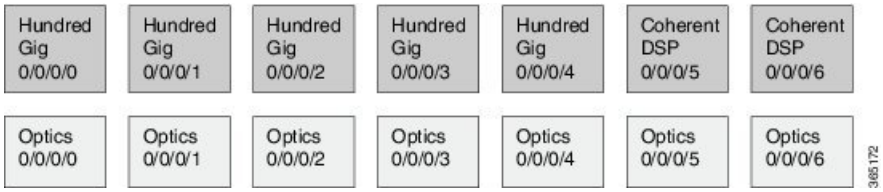
This chapter describes controllers such as Optics controller, Ethernet controller, and Coherent DSP Controller. This chapter also describes the procedures used to configure the controllers.

- Optics Controllers, on page 11
- Maintenance Mode, on page 12
- Configure Optics Controller, on page 12
- Configure Wavelength, on page 13
- Breakout Mode, on page 13
- Laser Squelching, on page 14
- LLDP Snooping, on page 14
- LLDP Snoop and Drop, on page 16
- Configure Ethernet Controller, on page 19
- Configure the Coherent DSP Controller, on page 20
- Configure Loopback, on page 20
- Restore Factory Settings, on page 21
- Headless Mode, on page 21
- View the Headless Statistics, on page 21

Optics Controllers

Controllers are represented in the *Rack/Slot/Instance/Port* format; for example, 0/0/0/1. Each port has an optics controller that is created on startup. When the slice is provisioned using the **hw-module** command, client layer controllers are created on the associated client and trunk ports. For example, HundredGig Ethernet controllers and TenGig Ethernet controllers are created on the associated client ports depending on the slice configuration; the CoherentDSP controller is created on the associated trunk ports.

The following figure describes the controller representation when the client rate is 100G and the trunk rate is 250G.



Maintenance Mode

Controllers can be placed in maintenance mode. Use the **controller optics sec-admin-state maintenance** command to place controllers in maintenance mode.

Use the **show controllers** *controllertype Rack/Slot/Instance/Port* command to view client and trunk alarms. In maintenance mode, all alarms are suppressed and the **show alarms** command does not display alarm details. However, traffic is not affected in maintenance mode.

Configure Optics Controller

You can configure parameters such as high power threshold, maximum and minimum chromatic dispersion, and wavelength for Optics controller. To configure Optics controller, use the following commands.

configure

controller *controllertype Rack/Slot/Instance/Port*

rx-high-threshold *rx-high*

tx-high-threshold *tx-high*

cd-max *cd-max*

cd-min *cd-min*

dwdm-carrier {**100MHz-grid frequency** *frequency*} | {**50GHz-grid** [**frequency** *frequency* | **wavelength** *wavelength* | **itu-ch** *channel-number*]}

commit

Note To view wavelength and channel mapping for optics controllers, use the **show controllers optics** *R/S/I/P* **dwdm-carrier-map** command.

Example

The following is a sample in which the high power threshold is configured at the receive and transmit side, maximum and minimum chromatic dispersion is configured, and wavelength is configured in 50GHz grid spacing.

```
configure
controller optics 0/0/0/1
rx-high-threshold 200
tx-high-threshold 300
cd-max 10000
cd-min 2000
dwdm-carrier 50GHz-grid wavelength 1560200
commit
```

Associated Commands

- controller optics

- show controllers

Configure Wavelength

You can configure the wavelength on trunk ports. Before configuring wavelength, use the following command to determine the valid range of wavelength.

show controllers optics *Rack/Slot/Instance/Port* **dwdm-carrier-map**

Displays the wavelength and channel mapping for trunk optics controllers. See Show Controllers command to view the DWDM carrier map table.

To configure wavelength, use the following commands.

configure

controller optics *Rack/Slot/Instance/Port*

dwdm-carrier {**100MHz-grid frequency** *frequency*} | {**50GHz-grid** [**frequency** *frequency* | **wavelength** *wavelength* | **itu-ch** *channel-number*]}

commit

In 50GHz grid spacing, enter the 7-digit wavelength value in the range of 1528773 to 1568362 nm. For example, enter 1532290 to specify 1532.29 nm. In 100MHz grid spacing, enter the 8-digit wavelength value in the range of 15667227 to 15287730 nm. For example, enter 15667227 to specify 1566.7227 nm.

Example

The following is a sample in which the wavelength is configured on the trunk port in 50GHz grid spacing.

```
show controllers optics 0/0/0/11 dwdm-carrier-map
configure
controller optics 0/0/0/0
dwdm-carrier 50GHz-grid wavelength 1560200
commit
```

Associated Commands

- dwdm-carrier
- show controllers

Breakout Mode

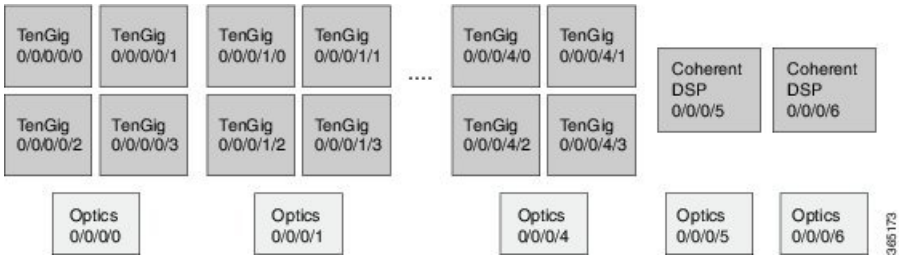
The client port can be enabled in normal mode or breakout mode. When the client bitrate is 10G, the mode is breakout mode.

RP/0/RP0/CPU0:ios(config)# **hw-module location 0/RP0/CPU0 slice 1 client bitrate 10g trunk bitrate 100g**

The client ports can operate at 10G mode using the breakout cable or the breakout patch panel. All five client ports of the slice need to be configured at the same bitrate. The controllers are represented in the

Rack/Slot/Instance/Port/Lanenumber format; for example, 0/0/0/1/3. The range of *Lanenumber* is from 1 to 4.

Four TenGig Ethernet controllers are created for each client port in breakout mode. The following figure describes the controller representation when the client rate is 10G and the trunk rate is 100G.



When the optics controller is shutdown, all four TenGig Ethernet controllers are shut down. Individual 10G port can be turned off from the TenGig Ethernet controller.

Laser Squelching

Ethernet controllers can be configured to enable laser squelching so that laser is brought down in the event of trunk faults (LOS, LOF) and a SQUELCHED alarm is raised. For 10G Ethernet controllers, laser squelching is supported only on LR4 and QSFP+ pluggables. For more information on SQUELCHED alarm, see the *Troubleshooting Guide for Cisco NCS 1000 Series, IOS XR Release 6.0.x*.

LLDP Snooping

Link Layer Discovery Protocol (LLDP) Snooping is enabled by default on all Ethernet controllers. The user can use LLDP snooping to troubleshoot problems in the client ports.

show controllers *controllertype Rack/Slot/Instance/Port* **lldp-snoop**

Note LLDP snoop and drop is not supported for VLAN-tagged LLDP packets.

Note If mandatory TLVs (Chassis ID, Port ID and TTL) are invalid or not available, then the LLDP neighbor information does not populate the LLDP packet details. The hardware drops the LLDP packet if LLDP drop is enabled.

Verify that the MAC address displayed is same as the MAC address of the traffic generating port. In Release 6.0.1, you can view more details about the LLDP neighbor.

```
RP/0/RP0/CPU0:ios# show controllers hundredGigECtrlr 0/0/0/8 lldp-snoop
Mon Apr  2 04:37:25.603 UTC

         LLDP Neighbor Snoop Data
-----------------------------------------------
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
```

```
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Local Controller:     HundredGigECtrlr0/0/0/8

Source MAC Address:   0010.9400.0002

Chassis ID:           ABCD

Port ID:              192.0.2.254

Port Description:     descr:ABCD Port-iter2

System Name:          Name:ABCD

System Description:   descr:ABCD-iter2

Hold Time(TTL):       120 seconds

System Capabilities:  P,B,W,R,T,C

Enabled Capabilities: P,R,T

Management Address:
        IPv4 address: 192.0.2.254
```

To verify the LLDP neighbor entries, use the following command:

```
RP/0/RP0/CPU0:ios# show lldp neighbors
Thu Jul 26 15:08:27.943 IST
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
Hav             EC0/0/0/4           120        B,R             Ethernet1/1

Total entries displayed: 1
```

EC refers to Ethernet Controller.

To display detailed information about LLDP neighbor entries, use the following command:

```
RP/0/RP0/CPU0:ios# show lldp neighbors detail
Thu Jul 26 15:08:03.836 IST
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

------------------------------------------------
Local Interface: HundredGigECtrlr0/0/0/4
Chassis id: a89d.21f8.4aa8
Port id: Ethernet1/1
Port Description: Ethernet1/1
System Name: Hav

System Description:
Cisco Nexus Operating System (NX-OS) Software 7.0(3)I4(7)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

Time remaining: 103 seconds
Hold Time: 120 seconds
System Capabilities: B,R
Enabled Capabilities: B,R
```

```
Management Addresses:
  IPv4 address: 10.77.132.26

Peer MAC Address: a8:9d:21:f8:4a:a8


Total entries displayed: 1
```

To clear LLDP neighbor snoop data, use the following command:

```
RP/0/RP0/CPU0:ios# clear controller hundredGigECtrlr 0/0/0/4  lldp-snoop
```

The **show lldp neighbors** command is supported for mac-sec- encrypt mode as well. Following is a sample output for 10GE mac-sec slice: Slice0, Slice3 in 10g client and 100g trunk with encrypt mode.

```
RP/0/RP0/CPU0:ios# show lldp neighbors
Fri Feb  3 13:21:09.779 IST
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
Spirent Test Center2 EC0/0/0/11/1          60         R,S            0194.3333.3333
Spirent Test Center2 EC0/0/0/11/2          60         R,S            0194.5555.5555
Spirent Test Center2 EC0/0/0/11/3          60         R,S            0194.2020.2121
Spirent Test Center2 EC0/0/0/11/4          60         R,S            0194.8888.8888
ROSCO NCS1K EC0/0/0/25/2                   60         P,R,S          0194.4444.4444
Spirent Test Center2 EC0/0/0/25/2          60         R,S            0194.6666.6666
Spirent Test Center2 EC0/0/0/25/3          27         R,S            0194.0000.0001
Spirent Test Center2 EC0/0/0/25/4          60         R,S            0194.0000.0011
```

LLDP Snoop and Drop

LLDP Drop feature is implemented in Release 6.1.2. Cisco NCS 1002 snoops the LLDP packets at each client controller port of a slice and drops the LLDP frame in the same slice without forwarding it to the peer slice.

Limitation:

LLDP Drop functionality with MACSEC encryption on NCS 1002 is not supported in Release 6.1.2 or earlier. Hence, it is not recommended to configure LLDP Drop functionality with MACSEC encryption in these releases. The LLDP snoop does not work for VLAN tagged LLDP packets, and hence the LLDP drop functionality does not occur.

Note If LLDP drop is disabled, slices perform legacy snoop and forward functionality by simply snooping and forwarding the LLDP frames to their peer slice.

Prerequisites:

Slices should be provisioned with client/trunk rate and should indicate *Provisioned* as status.

Configuring Slices and LLDP Drop at Slice Level

You can configure the slices and LLDP drop at a single slice, or over all slices. When the LLDP drop is enabled at slice then its corresponding client controller ports will also be enabled. By default, LLDP drop status is set to False. On enabling the LLDP Drop, its status is set to True.

To enable LLDP drop at single slice, use the following commands:

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate** { **10G | 40G | 100G** } **trunk bitrate** { **100G | 200G | 250G** } **fec** { **softdecision7 | softdecision20** }

hw-module location *location* **slice** *slice_number* **drop-lldp**

commit

Example:

To enable LLDP drop at slice 0, use the following commands.

```
RP/0/RP0/CPU0:ios(config)# hw-module location 0/RP0/CPU0 slice 0 client bitrate 40G trunk
bitrate 200G fec softDecision7
RP/0/RP0/CPU0:ios(config)# hw-module location 0/RP0/CPU0 slice 0 drop-lldp
RP/0/RP0/CPU0:ios(config)# commit
```

To enable LLDP drop over all slices, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate** { **10G | 40G | 100G** } **trunk bitrate** { **100G | 200G | 250G** } **fec** { **softdecision7 | softdecision20** } [**encrypted**]

hw-module location *location* **slice all drop-lldp**

commit

Example:

To enable LLDP drop over all slices, use the following commands.

```
RP/0/RP0/CPU0:ios(config)# hw-module location 0/RP0/CPU0 slice all client bitrate 40G trunk
 bitrate 200G fec softDecision7
RP/0/RP0/CPU0:ios(config)# hw-module location 0/RP0/CPU0 slice all drop-lldp
RP/0/RP0/CPU0:ios(config)# commit
```

Note You can configure LLDP drop for either on a single slice or over all slices. Both configuration commands cannot be executed together.

Associated Commands

- hwmodule
- show controllers

Verifying the Status of LLDP Drop

To verify the LLDP drop status of a slice, use the following command.

show hw-module { **slice** *slicenumber* | **all** | **fpd** }

Example:

The following is a sample in which the slice 0 is configured with 40G client bitrate, 200G trunk bitrate and LLDP drop is enabled.

```
RP/0/RP0/CPU0:ios(config)# show hw-module slice 0
Thu Sep 22 10:55:35.985 UTC
Slice ID:                0
Status:                  Provisioned
Client Bitrate:          40
Trunk Bitrate:           200
DP FPGA FW Type:         XMG4
DP FPGA FW Version:      01.01
HW Status:               CURRENT
Encryption Supported:    FALSE
LLDP Drop Enable: TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/6
Traffic Split Percentage
FortyGigECtrlr0/0/0/0                            100
FortyGigECtrlr0/0/0/1                            100
FortyGigECtrlr0/0/0/2                            100
FortyGigECtrlr0/0/0/3                            100
FortyGigECtrlr0/0/0/4                            100
```

To verify the LLDP drop status at the client controller level, use the following command.

show controllers *controllertype Rack/Slot/Instance/Port* **lldp-snoop**

Example :

The following is a sample in which the LLDP Drop is enabled for Forty GigE controller.

Note You can use respective controller type as per slice configuration (10/40/100).

```
RP/0/RP0/CPU0:ios(config)# show controllers FortyGigECtrlr 0/0/0/0 lldp-snoop
Thu Apr 28 09:49:20.684 UTC
Capability codes:R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
LLDP Neighbor Snoop Data
Local Controller:     FortyGigECtrlr0/0/0/0
Source MAC Address:   0010.9400.0044
Chassis ID:           192.0.2.10
Port ID:              0010.9400.0044
Port Description:     Spirent Port ROSCO
System Name:          Spirent Test CenterROSCO1111111111111
System Description:   Spirent Test Center ddddddddddddd
Hold Time(TTL):       20 seconds
System Capabilities:  R
Enabled Capabilities: R
Management Address:
IPv4 address: 192.0.2.10
LLDP Packet Drop enabled: TRUE
RX LLDP Packet Count : 1
```

Note RX LLDP Packet count represents the total number of packets received at the ingress of the Ethernet controller.

Disabling LLDP Drop

To disable LLDP drop, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **drop-lldp**

commit

Example:

To disable LLDP drop at slice 0, use the following commands.

```
RP/0/RP0/CPU0:ios(config)# no hw-module location 0/RP0/CPU0 slice 0 drop-lldp
RP/0/RP0/CPU0:ios(config)# commit
```

Once you disable LLDP Drop, show hw-module slice X and show controllers commands would display LLDP DROP ENABLED as FALSE.

Note When you disable LLDP Drop at slice level its corresponding client controller ports will also be disabled.

Configure Ethernet Controller

You can configure parameters such as performance monitoring, administrative state, laser squelching, and FEC for the Ethernet controller. To configure the Ethernet controller, use the following commands.

configure

controller *controllertype Rack/Slot/Instance/Port*

perf-mon { **enable** | **disable** }

sec-admin-state *admin-state*

laser-squelch

fec { **none** | **standard** }

commit

Example

The following is a sample in which the performance monitoring is enabled for HundredGig Ethernet controller, administrative state is placed under maintenance, laser squelching is enabled, and standard FEC is enabled.

```
configure
controller HundredGigECtrlr 0/0/0/0
perf-mon enable
sec-admin-state maintenance
laser-squelch
fec standard
commit
```

Associated Commands

- controller GigECtrlr
- show controllers

Configure the Coherent DSP Controller

You can configure parameters such as performance monitoring, administrative state, and trail trace identifier (TTI) for the Coherent DSP controller. In Release 6.0, the Coherent DSP is provisioned per slice, from Release 6.0.1, the Coherent DSP is provisioned per port. To configure the Coherent DSP controller, use the following commands.

configure

controller *controllertype Rack/Slot/Instance/Port*

perf-mon { **enable** | **disable** }

sec-admin-state *admin-state*

tti { **sent** | **expected** } **ascii** *string*

commit

Example

The following is a sample in which the performance monitoring is enabled for Coherent DSP controller, administrative state is placed under maintenance, and tti is configured.

```
configure
controller coherentDSP 0/0/0/12
perf-mon enable
sec-admin-state maintenance
tti sent ascii joy
commit
```

Associated Commands

- controller coherentDSP
- show controllers

Configure Loopback

You can configure the loopback on the CoherentDSP and Ethernet controllers. The loopback can be performed only in maintenance mode. Use the **controller optics sec-admin-state maintenance** command to place the controllers in maintenance mode. The line loopback on the tenGig Ethernet controller does not work when the port is squelched. To configure the loopback, use the following commands.

configure

controller *controllertype Rack/Slot/Instance/Port* **loopback** [**line** | **internal**]

commit

Example

The following is a sample in which the line loopback is configured on the Ethernet controller.

```
configure
controller HundredGigECtrlr 0/0/0/0 loopback line
commit
```

Associated Commands

- controller optics
- controller GigECtrlr
- controller coherentDSP

Restore Factory Settings

You can restore factory settings. The **commit replace** command replaces the entire running configuration with the contents of the target configuration. If the target configuration is empty, all existing configurations are removed and NCS 1002 will be restored to factory configuration. To restore NCS 1002 to factory settings, use the following commands.

configure

commit replace

Example

```
configure
commit replace
```

Headless Mode

NCS 1002 can carry traffic with a non-functional CPU (headless mode) for up to 72 hours. The data path and cumulative statistics are maintained for up to 72 hours with a non-functional CPU. The fault propagation continues to operate for failures on client and trunk ports. However, the provisioning operations cannot be performed and operational data cannot be viewed with a non-functional CPU. Performance monitoring data based on 15 minutes and 24 hour intervals is not supported with a non-functional CPU. In case of CPU OIR, the CPU needs to be physically replaced within 10 minutes.

View the Headless Statistics

Use this procedure to display the statistics collected during the last headless operation.

show controllers *controllertype R/S/I/P* **headless-stats**

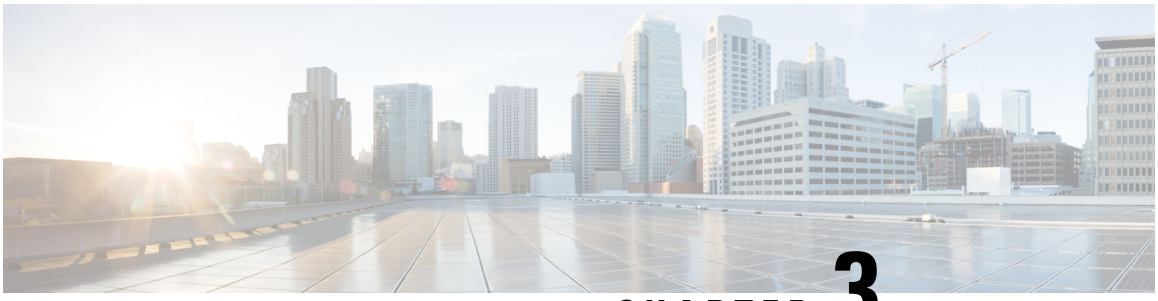
Example:

```
RP/0/RP0/CPU0:ios# show controllers hundredGigECtrlr 0/0/0/11 headless-stats
```

Displays the statistics collected during the last headless operation. The collected statistics is preserved for a slice until the hw-module configuration is removed or changed on that slice or until the next headless operation. The statistics is also preserved across process restarts.

Associated Commands

- show controllers



CHAPTER 3

Configuring IP Access List

This chapter describes how to configure IPv4 and IPv6 ACL.

- Configure IP Accesss List, on page 23

Configure IP Accesss List

To configure the ACL, use the following configuration at the IPv4 or IPv6 interface:

configure

interface *interface-type Rack/Slot/Instance/Port*

ipv4 | ipv6 access-group *access-list-name* **{ingress | egress}**

commit

Example

```
interface MgmtEth0/RP0/CPU0/0
ipv4 address 10.1.1.1 255.255.255.0
ipv6 address 1000::1/64
ipv4 access-group IPV4_ICMP_DENY ingress
ipv4 access-group IPV4_ROUTER_FWD_TELNET_TRAFFIC_DENY egress
ipv6 access-group IPV6_SSH_DENY ingress
ipv6 access-group IPV6_ROUTER_FWD_TELNET_TRAFFIC_DENY egress
```

Sample Configuration for IPv4 Access Lists

```
ipv4 access-list IPV4_ICMP_DENY
10 deny icmp any any
20 permit ipv4 any any
!
ipv4 access-list IPV4_ROUTER_FWD_TELNET_TRAFFIC_DENY
10 deny tcp any any eq telnet
20 permit ipv4 any any
!
```

Sample Configuration for IPv6 Access Lists

```
ipv6 access-list IPV6_SSH_DENY
10 deny tcp any any eq ssh
20 permit ipv6 any any
!
ipv6 access-list IPV6_ROUTER_FWD_TELNET_TRAFFIC_DENY
10 deny tcp any any eq telnet
```

```
20 permit ipv6 any any
!
```

Verify IPv6 ACL

The following examples verify the number of packets filter by respecitve ACLs:

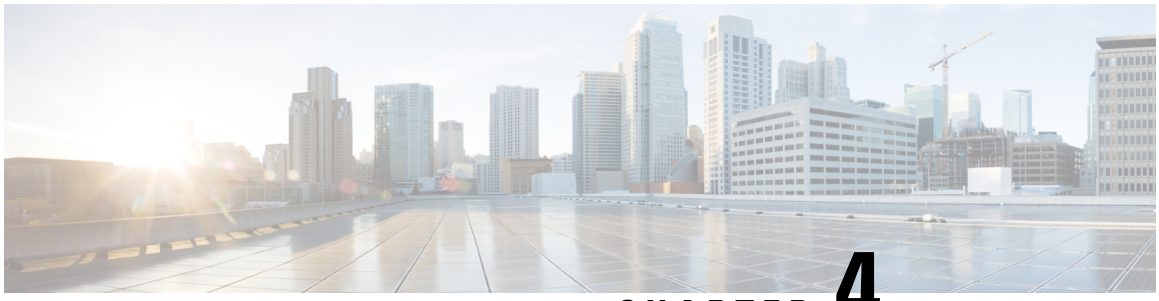
Examples to check statistics

RP/0/RP0/CPU0:ios#**show access-lists ipv4**

```
Wed Jan 17 09:52:12.448 IST
ipv4 access-list IPV4_ICMP_DENY
10 deny icmp any any (8 matches)
20 permit ipv4 any any (106 matches)
ipv4 access-list IPV4_ROUTER_FWD_TELNET_TRAFFIC_DENY
10 deny tcp any any eq telnet (3 matches)
20 permit ipv4 any any (6 matches)
```

RP/0/RP0/CPU0:ios#**show access-lists ipv6**

```
Wed Jan 17 09:52:14.591 IST
ipv6 access-list IPV6_ROUTER_FWD_TELNET_TRAFFIC_DENY
10 deny tcp any any eq telnet (3 matches)
20 permit ipv6 any any (5 matches)
ipv6 access-list IPV6_SSH_DENY
10 deny tcp any any eq ssh (9 matches)
20 permit ipv6 any any (100 matches)
RP/0/RP0/CPU0:PROD_20#
```



CHAPTER 4

Configuring Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for, and report performance data for early detection of problems. The user can retrieve both current and historical PM counters for the various controllers in 15 minutes and 1 day intervals.

PM for optical parameters include laser bias current, transmit and receive optical power, mean polarization mode dispersion, accumulated chromatic dispersion, and received optical signal-to-noise ratio (OSNR). These parameters simplify troubleshooting operations and enhance data that can be collected directly from the equipment.

Note The supported MTU of data plane is as follows:

- Range: 60 bytes to 10 kilobytes
- Jumbo: 10 kilobytes
- Undersize: 60 to 64 bytes

For descriptions of optics, Ethernet, fec, and otn parameters, see the *Command Reference for Cisco NCS 1000 Series*.

- Configure PM Parameters, on page 25
- View PM Parameters, on page 27
- Pseudo Random Binary Sequence, on page 31

Configure PM Parameters

You can configure the performance monitoring parameters for the Optics, Ethernet, and coherent DSP controllers. The coherent DSP controller is created on the trunk port when the slice is provisioned using the **hw-module** command. To configure PM parameters, use the following commands.

configure

commit

Examples

The following is a sample in which the performance monitoring parameters of Optics controller is configured in 24 hour intervals.

```
configure
controller optics 0/0/0/0 pm 24-hour optics report cd max-tca enable
commit
```

The following is a sample in which the performance monitoring parameters of Ethernet controller is configured in 15 minute intervals.

```
configure
controller HundredGigECtrlr 0/0/0/1 pm 15-min ether report 1024-1518-octets enable
commit
```

The following is a sample in which the performance monitoring parameters of Coherent DSP controller is configured in 15 minute intervals.

```
configure
controller coherentDSP 0/0/0/12 pm 15-min otn threshold es-ne
commit
```

Configure FEC BER Thresholds

Pre-forward error correction (FEC) bit error rate (BER) or post-FEC BER values are represented in numerical values. BER value is multiplied by 1E-15 to derive numerical value. For example, 2.1e-4 is displayed as 210000000000(2.1e+11).

The following is a sample to enable minimum and maximum TCAs for pre-FEC BER.

```
configure
controller coherentDSP 0/0/0/6 pm 30-sec fec report pre-fec-ber min-tca enable
controller coherentDSP 0/0/0/6 pm 30-sec fec report pre-fec-ber max-tca enable
commit
```

The following is a sample to enable minimum and maximum TCAs for post-FEC BER.

```
configure
controller coherentDSP 0/0/0/6 pm 30-sec fec report post-fec-ber min-tca enable
controller coherentDSP 0/0/0/6 pm 30-sec fec report post-fec-ber max-tca enable
commit
```

The following is a sample to configure pre-FEC BER thresholds of Coherent DSP controller in 30 second intervals.

```
configure
controller coherentDSP 0/0/0/6 pm 30-sec fec threshold pre-fec-ber max 320000000000
commit
```

The following is a sample to configure post-FEC BER thresholds of Coherent DSP controller in 30 second intervals.

```
configure
controller coherentDSP 0/0/0/6 pm 30-sec fec threshold post-fec-ber max 320000000000
commit
```

The following is a sample of the show controllers command.

```
show controllers coherentDSP 0/0/0/6 pm current 30-sec fec

Mon Feb 25 05:29:20.980 UTC

g709 FEC in the current interval [05:29:00 - 05:29:21 Mon Feb 25 2019]

FEC current bucket type : Valid
    EC-BITS   : 1196208549              Threshold : 903330                TCA(enable)  :
NO
    UC-WORDS  : 0                       Threshold : 5                     TCA(enable)  :
YES

                MIN       AVG        MAX    Threshold   TCA     Threshold   TCA
                                              (min)    (enable)   (max)    (enable)
PreFEC BER  :   0E-15     0E-15     0E-15       0        NO   320000000000       YES
PostFEC BER :   0E-15     0E-15     0E-15       0        NO   320000000000       YES
```

Associated Commands

- pm
- controller optics
- controller GigECtrlr
- controller coherentDSP
- show controllers

View PM Parameters

Use this procedure to view the performance monitoring parameters for Optics, Ethernet, and coherent DSP controllers.

Example:

```
RP/0/RP0/CPU0:ios# show controllers optics 0/0/0/1 pm current 15-min optics 1
```

Displays the current performance monitoring parameters of the Optics controller in 15 minute intervals.

Client optics has four lanes and trunk optics has one lane.

```
Fri Aug 21 09:28:57.608 UTC

Optics in the current interval [ 9:15:00 - 09:28:57 Fri Aug 21 2015]

Optics current bucket type : Valid
             MIN       AVG       MAX     Threshold  TCA     Threshold  TCA
                                          (min)    (enable)    (max)    (enable)
LBC[% ]     : 0.0       0.0       0.0       0.0      NO        0.0      NO
OPT[dBm]    : -inf      -inf      -inf      0.00     NO        0.00     NO
OPR[dBm]    : -inf      -inf      -inf      0.00     NO        0.00     NO

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

Example:

```
RP/0/RP0/CPU0:ios# show controllers hundredGigECtrlr 0/0/0/3 pm current 15-min ether
```

Displays the current performance monitoring parameters of the Ethernet controller in 15 minute intervals.

```
Mon Jan 28 07:20:28.170 IST

ETHER in the current interval [07:15:00 - 07:20:29 Mon Jan 28 2019]

ETHER current bucket type : Valid
RX-UTIL[%]                : 2.90                Threshold : 0.00         TCA(enable) : NO
TX-UTIL[%]                : 2.84                Threshold : 0.00         TCA(enable) : NO
RX-PKT                    : 78662810            Threshold : 0            TCA(enable) : NO
STAT-PKT                  : 0                   Threshold : 0            TCA(enable) : NO
OCTET-STAT                : 117994199787        Threshold : 0            TCA(enable) : NO
OVERSIZE-PKT              : 0                   Threshold : 0            TCA(enable) : NO
FCS-ERR                   : 0                   Threshold : 0            TCA(enable) : NO
LONG-FRAME                : 0                   Threshold : 0            TCA(enable) : NO
JABBER-STATS              : 0                   Threshold : 0            TCA(enable) : NO
64-OCTET                  : 0                   Threshold : 0            TCA(enable) : NO
65-127-OCTET              : 0                   Threshold : 0            TCA(enable) : NO
128-255-OCTET             : 0                   Threshold : 0            TCA(enable) : NO
256-511-OCTET             : 0                   Threshold : 0            TCA(enable) : NO
512-1023-OCTET            : 0                   Threshold : 0            TCA(enable) : NO
1024-1518-OCTET           : 0                   Threshold : 0            TCA(enable) : NO
IN-UCAST                  : 78662799            Threshold : 0            TCA(enable) : NO
IN-MCAST                  : 11                  Threshold : 0            TCA(enable) : NO
IN-BCAST                  : 0                   Threshold : 0            TCA(enable) : NO
OUT-UCAST                 : 0                   Threshold : 0            TCA(enable) : NO
OUT-BCAST                 : 0                   Threshold : 0            TCA(enable) : NO
OUT-MCAST                 : 0                   Threshold : 0            TCA(enable) : NO
TX-PKT                    : 76889333            Threshold : 0            TCA(enable) : NO
OUT-OCTET                 : 115333999500        Threshold : 0            TCA(enable) : NO
IFIN-ERRORS               : 0                   Threshold : 0            TCA(enable) : NO
IFIN-OCTETS               : 0                   Threshold : 0            TCA(enable) : NO
STAT-MULTICAST-PKT        : 0                   Threshold : 0            TCA(enable) : NO
STAT-BROADCAST-PKT        : 0                   Threshold : 0            TCA(enable) : NO
STAT-UNDERSIZED-PKT       : 0                   Threshold : 0            TCA(enable) : NO
IN_GOOD_BYTES             : 117994199787        Threshold : 0            TCA(enable) : NO
IN_GOOD_PKTS              : 78662810            Threshold : 0            TCA(enable) : NO
IN_DROP_OTHER             : 0                   Threshold : 0            TCA(enable) : NO
IN_ERROR_FRAGMENTS        : 0                   Threshold : 0            TCA(enable) : NO
IN_PKT_64_OCTET           : 0                   Threshold : 0            TCA(enable) : NO
IN_PKTS_65_127_OCTETS     : 11                  Threshold : 0            TCA(enable) : NO
IN_PKTS_128_255_OCTETS    : 0                   Threshold : 0            TCA(enable) : NO
IN_PKTS_256_511_OCTETS    : 0                   Threshold : 0            TCA(enable) : NO
IN_PKTS_512_1023_OCTETS   : 0                   Threshold : 0            TCA(enable) : NO
IN_PKTS_1024_1518_OCTETS  : 78662799            Threshold : 0            TCA(enable) : NO
TX_UNDERSIZED_PKT         : 0                   Threshold : 0            TCA(enable) : NO
TX_OVERSIZED_PKT          : 0                   Threshold : 0            TCA(enable) : NO
TX_FRAGMENTS              : 0                   Threshold : 0            TCA(enable) : NO
TX_JABBER                 : 0                   Threshold : 0            TCA(enable) : NO
TX_BAD_FCS                : 0                   Threshold : 0            TCA(enable) : NO

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

Example:

```
RP/0/RP0/CPU0:ios# show controllers coherentDSP 0/0/0/13 pm current 15-min otn
```

Displays the current performance monitoring parameters of the Coherent DSP controller in 15 minute intervals.

```
Tue Feb 13 15:43:00.173 UTC

g709 OTN in the current interval [15:30:00 - 15:43:00 Tue Feb 13 2001]
```

```
OTN current bucket type : Valid
    ES-NE   : 0         Threshold : 500      TCA(enable)  : YES
    ESR-NE  : 0.00000   Threshold : 0.00000  TCA(enable)  : NO
    SES-NE  : 0         Threshold : 500      TCA(enable)  : YES
    SESR-NE : 0.00000   Threshold : 0.00000  TCA(enable)  : NO
    UAS-NE  : 0         Threshold : 500      TCA(enable)  : YES
    BBE-NE  : 0         Threshold : 10000    TCA(enable)  : YES
    BBER-NE : 0.00000   Threshold : 0.00000  TCA(enable)  : NO
    FC-NE   : 0         Threshold : 10       TCA(enable)  : YES

    ES-FE   : 0         Threshold : 500      TCA(enable)  : YES
    ESR-FE  : 0.00000   Threshold : 0.00000  TCA(enable)  : NO
    SES-FE  : 0         Threshold : 500      TCA(enable)  : YES
    SESR-FE : 0.00000   Threshold : 0.00000  TCA(enable)  : NO
    UAS-FE  : 0         Threshold : 500      TCA(enable)  : YES
    BBE-FE  : 0         Threshold : 10000    TCA(enable)  : YES
    BBER-FE : 0.00000   Threshold : 0.00000  TCA(enable)  : NO
    FC-FE   : 0         Threshold : 10       TCA(enable)  : YES

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

Example:

```
RP/0/RP0/CPU0:ios# show controllers optics 0/0/0/0 pm current flex-bin optics 1


Mon Dec  7 15:57:42.886 IST

Optics in the current interval [15:57:40 - 15:57:42 Mon Dec 7 2020]

Flexible bin interval size: 10 seconds

Optics current bucket type : Valid
           MIN    AVG    MAX  Operational   Configured       TCA  Operational  Configured    TCA
                              Threshold(min)Threshold(min)   (min)Threshold(max)Threshold(max)(max)
LBC[% ]  : 53.0   53.0   53.0   0.0            NA           NO     0.0             NA          NO
OPT[dBm] : 0.91   0.92   0.92   0.00           NA           NO     0.00            NA          NO
OPR[dBm] : -0.46  -0.41  -0.38  0.00           NA           NO     0.00            NA          NO
Last clearing of "show controllers OPTICS" counters never
```

Example:

```
RP/0/RP0/CPU0:ios# show controllers hundredGigECtrlr 0/0/0/0 pm current flex-bin ether


Mon Dec  7 15:58:56.007 IST
ETHER in the current interval [15:58:50 - 15:58:55 Mon Dec 7 2020]
Flexible bin interval size: 10 seconds
ETHER current bucket type : Valid
 RX-UTIL[%]               : 4.89               Threshold : 0.00         TCA(enable) : NO
 TX-UTIL[%]               : 4.89               Threshold : 0.00         TCA(enable) : NO
 RX-PKT                   : 24828201           Threshold : 0            TCA(enable) : NO
 STAT-PKT                 : 0                  Threshold : 0            TCA(enable) : NO
 OCTET-STAT               : 3178009728         Threshold : 0            TCA(enable) : NO
 OVERSIZE-PKT             : 0                  Threshold : 0            TCA(enable) : NO
 FCS-ERR                  : 0                  Threshold : 0            TCA(enable) : NO
 LONG-FRAME               : 0                  Threshold : 0            TCA(enable) : NO
 JABBER-STATS             : 0                  Threshold : 0            TCA(enable) : NO
 64-OCTET                 : 0                  Threshold : 0            TCA(enable) : NO
 65-127-OCTET             : 0                  Threshold : 0            TCA(enable) : NO
 128-255-OCTET            : 0                  Threshold : 0            TCA(enable) : NO
 256-511-OCTET            : 0                  Threshold : 0            TCA(enable) : NO
 512-1023-OCTET           : 0                  Threshold : 0            TCA(enable) : NO
 1024-1518-OCTET          : 0                  Threshold : 0            TCA(enable) : NO
 IN-UCAST                 : 24828201           Threshold : 0            TCA(enable) : NO
 IN-MCAST                 : 0                  Threshold : 0            TCA(enable) : NO
```

```
 IN-BCAST                  : 0                    Threshold : 0            TCA(enable) : NO
 OUT-UCAST                 : 0                    Threshold : 0            TCA(enable) : NO
 OUT-BCAST                 : 0                    Threshold : 0            TCA(enable) : NO
 OUT-MCAST                 : 0                    Threshold : 0            TCA(enable) : NO
 TX-PKT                    : 24826715             Threshold : 0            TCA(enable) : NO
 OUT-OCTET                 : 3177819520           Threshold : 0            TCA(enable) : NO
 IFIN-ERRORS               : 0                    Threshold : 0            TCA(enable) : NO
 IFIN-OCTETS               : 0                    Threshold : 0            TCA(enable) : NO
 STAT-MULTICAST-PKT        : 0                    Threshold : 0            TCA(enable) : NO
 STAT-BROADCAST-PKT        : 0                    Threshold : 0            TCA(enable) : NO
 STAT-UNDERSIZED-PKT       : 0                    Threshold : 0            TCA(enable) : NO
 IN_GOOD_BYTES             : 3178009728           Threshold : 0            TCA(enable) : NO
 IN_GOOD_PKTS              : 24828201             Threshold : 0            TCA(enable) : NO
 IN_DROP_OTHER             : 0                    Threshold : 0            TCA(enable) : NO
 OUT_GOOD_BYTES            : 0                    Threshold : 0            TCA(enable) : NO
 OUT_GOOD_PKTS             : 0                    Threshold : 0            TCA(enable) : NO
 IN_ERROR_FRAGMENTS        : 0                    Threshold : 0            TCA(enable) : NO
 IN_PKT_64_OCTET           : 0                    Threshold : 0            TCA(enable) : NO
 IN_PKTS_65_127_OCTETS     : 0                    Threshold : 0            TCA(enable) : NO
 IN_PKTS_128_255_OCTETS    : 24828201             Threshold : 0            TCA(enable) : NO
 IN_PKTS_256_511_OCTETS    : 0                    Threshold : 0            TCA(enable) : NO
 IN_PKTS_512_1023_OCTETS   : 0                    Threshold : 0            TCA(enable) : NO
 IN_PKTS_1024_1518_OCTETS  : 0                    Threshold : 0            TCA(enable) : NO
 TX_UNDERSIZED_PKT         : 0                    Threshold : 0            TCA(enable) : NO
 TX_OVERSIZED_PKT          : 0                    Threshold : 0            TCA(enable) : NO
 TX_FRAGMENTS              : 0                    Threshold : 0            TCA(enable) : NO
 TX_JABBER                 : 0                    Threshold : 0            TCA(enable) : NO
 TX_BAD_FCS                : 0                    Threshold : 0            TCA(enable) : NO

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

Example:

```
RP/0/RP0/CPU0:ios# show controllers coherentDSP 0/0/0/5 pm current flex-bin fec


Mon Dec  7 16:00:20.005 IST
g709 FEC in the current interval [16:00:10 - 16:00:19 Mon Dec 7 2020]
Flexible bin interval size: 10 seconds
FEC current bucket type : Valid
    EC-BITS   : 24852481632            Threshold : 0                    TCA(enable)  : NO
    UC-WORDS  : 0                      Threshold : 0                    TCA(enable)  : NO

              MIN       AVG        MAX      Threshold   TCA   Threshold   TCA
                                  (min)     (enable)    (max)   (enable)
PreFEC BER    7.1E-03   7.7E-03    8.4E-03   0E-15       NO     0E-15      NO
PostFEC BER   0E-15     0E-15      0E-15     0E-15       NO     0E-15      NO
Last clearing of "show controllers OTU" counters never
```

Associated Commands

- pm
- show controllers
- controller optics
- controller GigECtrlr
- controller coherentDSP

Pseudo Random Binary Sequence

The Pseudo Random Binary Sequence (PRBS) feature allows you to perform data integrity checks between the NCS1002 trunk links without enabling the actual client traffic.

You can configure NCS 1002 trunk port in any one of the following modes for PRBS on the 1.2T card:

- **Source mode —** The NCS 1002 at trunk port generates PRBS signal on the line continuously as per the configured PRBS pattern.
- **Sink mode —** The NCS 1002 at trunk port gets locked to the ingress signal according to the configured pattern, analyzes and reports the errors.
- **Source-Sink mode —** The NCS 1002 at trunk port acts as both the PRBS transmitter and receiver, that is, it generates PRBS signal as per the configured pattern, and also gets locked to the ingress signal with the same pattern, and reports the errors.
- **PRBS31 —** Sequence length is from 2^31 -1 bits.
- **PRBS23 —** Sequence length is from 2^23 -1 bits.
- **PRBS15 —** Sequence length is from 2^15 -1 bits.
- **PRBS11 —**Sequence length is from 2^11 -1 bits.

Limitations of PRBS

There are following limitations with the PRBS feature:

- There is no SNMP support to fetch the PRBS status or Performance Monitoring (PM).
- 30-secs current/historic PMs are not supported for PRBS feature.
- PRBS PM TCAs are not supported.
- Apply PRBS configuration only after coherentDSP upgrade is complete.

Configuring Pseudo Random Binary Sequence

To enable the PRBS on the trunk port, use the following configuration command at the coherentDSP controller:

controller coherentDSP *R/S/I/P* **prbs mode** {**source | sink | source-sink**} **pattern** {**pn31 | pn23 | pn15 | pn11**}

When the PRBS is enabled on the trunk ports, you can view the following impacts in the corresponding client ports:

- Client traffic is dropped in the direction of source to sink as the frames are overwritten by the PRBS pattern.
- Remote fault is raised on the client ports nearer to the PRBS sink.
- Client ports on both the sides are squelched when PRBS is enabled on the trunks and when laser-squelch is configured on the clients.
- Line Loopback on the client ports works without any issues.

- Internal Loopback on the client ports does not work when PRBS is enabled on the trunk ports.

Viewing PRBS Performance Monitoring Parameters

PRBS PM parameters are not available for the controllers in Source mode. PRBS PM parameters are reset when PRBS configuration changes on the controller.

To view the PRBS PM parameters on the coherentDSP controller, use the following command:

show controllers coherentDSP | ODU4 *R/S/I/P* **pm** {**current | history** }{**15-min|24-hour**} **prbs**

```
RP/0/RP0/CPU0:PROD15#sh controllers coherentDSP 0/0/0/6 pm current 15-min prbs
Sat Jun 24 14:04:25.260 UTC
 PRBS in the current interval [14:00:00 - 14:04:25 Sat Jun 24 2017]
 PRBS current bucket type : Valid
 EBC          : 306
 FOUND-COUNT  : 5                    FOUND-AT-TS : 14:04:16 Sat Jun 24 2017
 LOST-COUNT   : 5                    LOST-AT-TS  : 14:04:10 Sat Jun 24 2017
 CONFIG-PTRN  : PRBS_PATTERN_PN31
 STATUS : LOCKED
Last clearing of "show controllers OTU" counters never
RP/0/RP0/CPU0:PROD15
```

The following tables describes the fields of PRBS PM parameters.

Table 2: PRBS PM Parameters

PM Parameter	Description
EBC	Cumulative count of PRBS bit errors in the sampling interval (15-minute or 24-hour). PRBS bit errors are accumulated only if PRBS signal is locked.
FOUND-COUNT	Number of state transitions from signal unlocked state to signal locked state in the sampling interval. If state change is not observed in the interval, the count is 0.
LOST-COUNT	Number of state transitions from signal locked state to signal unlocked state in the sampling interval. If state change is not observed in the interval, the count is 0.
FOUND-AT-TS	Latest timestamp when the PRBS state moves from unlocked state to locked state in the sampling interval. If state change is not observed in the interval, the value is null.
CONFIG-PTRN	Configured PRBS pattern on the port.

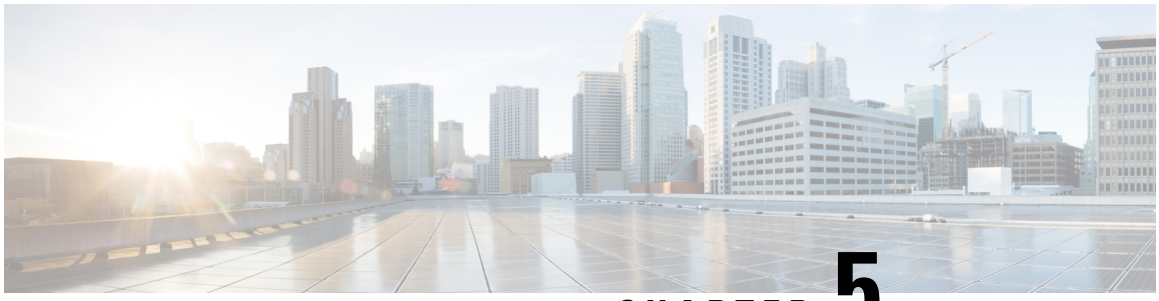
Verifying PRBS

R/S/I/P **prbs-details**

```
RP/0/RP0/CPU0:PROD15#show controllers coherentDSP 0/0/0/6 prbs-details
Sat Jun 24 13:28:57.549 UTC
 -------------------------PRBS details---------------------------------
```

```
PRBS Test               : Enable
PRBS Mode               : Source-Sink
PRBS Pattern            : PN31
PRBS Status             : Locked
------------------------------------------------
RP/0/RP0/CPU0:PROD15#
```

- You cannot view any details, if the PRBS is not enabled on the trunk.
- PRBS status is shown as **Not Applicable**, when the mode is **Source**.
- PRBS status is shown as **unlocked**, when the signal is not locked on the receiving side in the **Sink** or **Source-Sink** mode.



CHAPTER 5

Configuring MACsec Encryption

MAC Security (MACsec) is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec capable devices.

Security breaches can occur at any layer of the OSI model. Some of the common breaches at Layer 2 are MAC address spoofing, ARP spoofing, Denial of Service (DoS) attacks against a DHCP server, and VLAN hopping.

MACsec secures the data on physical media, making it impossible for data to be compromised at higher layers. As a result, MACsec encryption takes priority over any other encryption method for higher layers, such as IPsec and SSL.

MACsec provides encryption at the Layer 2, which is provided by the Advanced Encryption Standard (AES) algorithm that replaces the DES algorithm. MACsec uses the MACsec Key Agreement protocol (MKA) to exchange session keys, and manage encryption keys.

- MACsec Frame Format, on page 36
- MACsec SECTag Format , on page 37
- MACsec Key Agreement, on page 37
- MACsec in NCS 1002, on page 37
- Supported Configurations in Encrypted Mode, on page 38
- Illustrations for Supported Configurations in Encrypted Mode, on page 39
- Configure MACsec Encryption Using PSK Authenication, on page 40
- MACsec Key Chain, on page 40
- Configure MACsec Key Chain, on page 41
- Verify MACsec Key Chain, on page 42
- MACsec Policy, on page 43
- Configure MACsec Policy, on page 43
- Verify MACsec Policy, on page 45
- MACsec Controllers, on page 46
- Configure the Slice, on page 46
- Verify Slice Configuration, on page 48
- Apply MACsec Configuration on MACsec Controller, on page 51
- Verify MACsec Configuration on MACsec Controller, on page 52
- Verify State of MACSec Controller, on page 56

- SecY Statistics, on page 56
- Trunk Side Statistics, on page 59
- Control Plane Statistics, on page 60
- Configuring MACsec Threshold Crossing Alerts, on page 61
- View MACsec PM Parameters, on page 62
- MACsec MKA Using EAP-TLS Authentication , on page 68
- IEEE 802.1X Device Roles, on page 68
- Prerequisites for MACsec MKA Using EAP-TLS Authentication, on page 68
- Configure MACsec Encryption Using EAP-TLS Authentication, on page 69
- Configure RADIUS Server, on page 69
- Configure 802.1X Authentication Method, on page 70
- Generate RSA Key Pair, on page 71
- Configure Trust Point, on page 71
- Authenticate Certificate Authority and Request Certificates, on page 72
- Configure EAP Profile, on page 73
- Configure 802.1X Profile, on page 74
- Configure EAP and 802.1X Profile on MACsec Controller, on page 75
- Verify EAP and 802.1X Configuration on MACsec Controller, on page 76

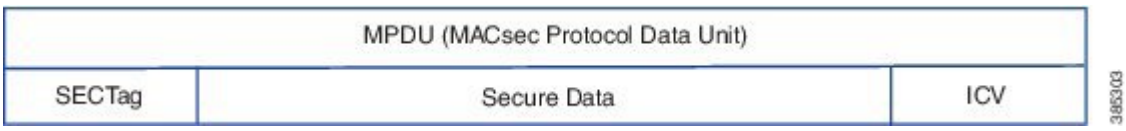
MACsec Frame Format

The MACsec header in a frame consists of three fields.

Table 3: Fields in MACsec Frame

Field	Size	Description
SECTag	8 or 16 bytes	Identifies the Security Association Key (SAK) to be used to validate the received frame. The security tag also provides replay protection when frames are received out of sequence. With Secure Channel Identifier (SCI) encoding, the security tag is 16 bytes in length, and without the encoding, 8 bytes in length (SCI encoding is optional).
Secure Data	2+ octets	Data in the frame that is encrypted using MACsec.
ICV	128 bit	Integrity Check Value (ICV) that provides the integrity check for the frame. Frames that do not match the expected ICV are dropped at the port.

Figure 2: MACsec Frame Format



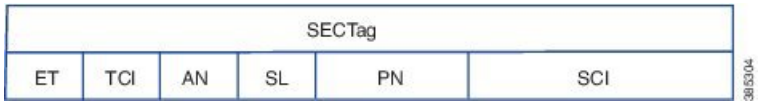
MACsec SECTag Format

The MACsec SECTag header in a frame consists of the following fields.

Table 4: Fields in MACsec SECTag Frame

Field	Size	Description
ET	16 bit	MACsec EtherType value (0x88E5) for MACsec packet.
TCI	6 bit	Tag control information that indicates how frame is protected.
AN	2 bit	Association number.
SL	8 bit	Short length of MAC service data unit (MSDU).
PN	32 bit	Packet sequence number.
SCI	64 bit	(optional) Secure channel identifier.

Figure 3: MACsec SECTag Frame Format



MACsec Key Agreement

The MACsec Key Agreement (MKA) Protocol, defined in IEEE 802.1X-2010, provides the required session keys and manages the required encryption keys. MKA is a multipoint to multipoint protocol that defines the mechanism to generate and distribute keys for MACsec.

MKA allows authorized multiple devices that possess secret key (CAK) to participate in a CA (Connectivity Association). It defines the election of Key Server (KS) that generates the Security Association Key(SAK) and distributes the SAK to all the participants. MACsec frames across the devices are secured using SAK. MKA also transports MACsec capability such as delay protection and confidentiality offset.

MKA operates in two modes.

- MKA using pre-shared key (PSK) authentication. See Configure MACsec Encryption Using PSK Authenication, on page 40 for configuration steps.
- MKA using Extensible Authentication Protocol (EAP) authentication. EAP mode uses 802.1X authentication. See Configure MACsec Encryption Using EAP-TLS Authentication, on page 69 for configuration steps.

MACsec in NCS 1002

MACsec in NCS 1002 has the following characteristics or limitations.

- Supports 256-bit Extended Packet Numbering (XPN) according to IEEE 802.1AEbn-2011.
- Supports GCM-AES-XPN-256 as the default cipher.
- Supports AES-128-CMAC and AES-256-CMAC cryptographic algorithms.
- Supports SecY function in the data plane as specified by IEEE 802.1 AE-2006 specification.
- Supports only 2 x 100G client and 1 x 200G trunk traffic.
- Supports only cumulative statistics for MACsec counters.
- Supported only with the ncs1k-k9sec package.
- Not supported in the headless mode.
- Recommended to upgrade the nodes to R6.2.1 and bring up the 100G MACsec sessions.
- For 100G MACsec deployed in R6.1.1 and R6.1.2: If the customer migrates from R6.1.2 to R6.2.1, traffic hit occurs. The subsequent headless operations will not have any traffic drops.

Note When the user needs to use the MACsec feature and upgrades from R6.0.1 to 6.1.1, the control FPGA (CTRL_BKP_UP, CTRL_BKP_LOW, CTRL_FPGA_UP, and CTRL_FPGA_LOW) needs to be upgraded to the latest firmware version provided by R6.1.1. See Verify Firmware Version for more information.

Supported Configurations in Encrypted Mode

The following configurations are supported on client and trunk ports in each slice configured in encrypted mode.

Client Ports	Trunk Ports
2 x 100G	1 x 200G
10 x 10G	1 x 100G
2 x 40G	1 x 100G

All the configurations can be accomplished using appropriate values for client bitrate and trunk bitrate parameters of the **hw-module** command.

The following table describes the client and trunk ports in slice 0 that are enabled or disabled for each supported configuration in encrypted mode.

Client Data Rate	Trunk Data Rate	Client Port 0	Client Port 1	Client Port 2	Client Port 3	Client Port 4	Trunk Port 5	Trunk Port 6
100G	200G	D	D	D	E	E	D	E

Client Data Rate	Trunk Data Rate	Client Port 0	Client Port 1	Client Port 2	Client Port 3	Client Port 4	Trunk Port 5	Trunk Port 6
10G	100G	D	D	Only the first and second controllers are active.	E	E	D	E
40G	100G	D	D	D	E	E	D	E

E indicates that the port is enabled; D indicates that the port is disabled.

Illustrations for Supported Configurations in Encrypted Mode

The following illustrations describe the mapping of traffic from client to trunk ports in encrypted mode for the supported configurations.

Figure 4: Client: 2 x 100G Trunk: 1 x 200G

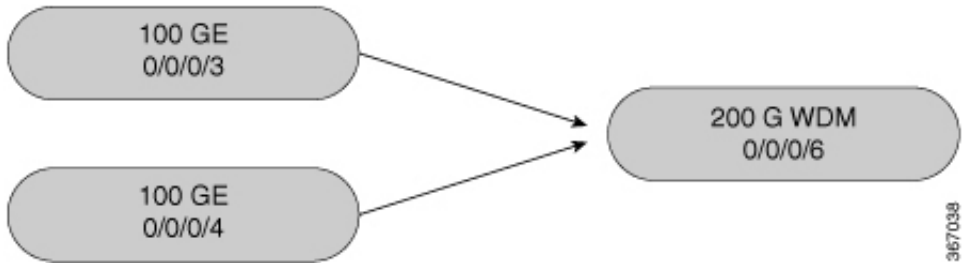


Figure 5: Client: 10 x 10G Trunk: 1 x 100G

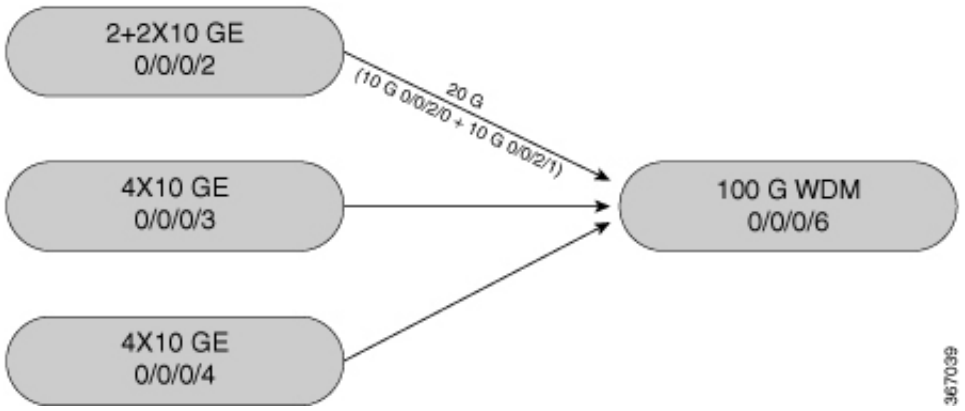
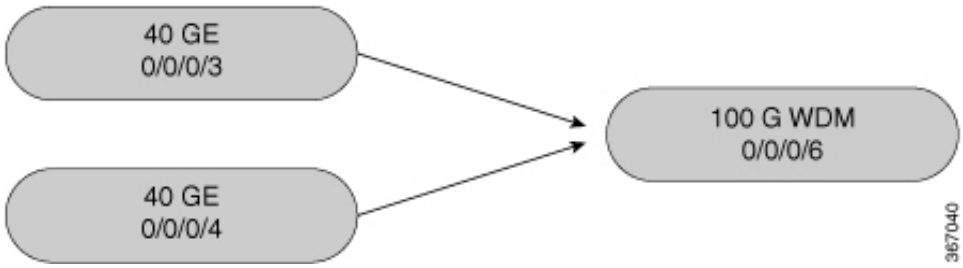


Figure 6: Client: 2 x 40G Trunk: 1 x 100G



Configure MACsec Encryption Using PSK Authenication

Configuring MACsec encryption using PSK authentication involves the following tasks:

1. Configure MACsec Key Chain, on page 41
2. Verify MACsec Key Chain, on page 42
3. Configure MACsec Policy, on page 43
4. Verify MACsec Policy, on page 45
5. Configure the Slice, on page 3
6. Verify Slice Configuration, on page 5
7. Apply MACsec Configuration on MACsec Controller, on page 51
8. Verify MACsec Configuration on MACsec Controller, on page 52

MACsec Key Chain

A MACsec key chain is a collection of keys used to authenticate peers needing to exchange encrypted information. While creating a key chain, we define the key(s), key string with password, the cryptographic algorithm, and the key lifetime.

- The key can be up to 64 characters in length.
- The key name must be of even number of characters. Entering an odd number of characters will exit the MACsec configuration mode. The key name must match on both the sides.
- The key string is 64 hexadecimal characters in length when AES 256-bit encryption algorithm is used and 32 hexadecimal characters in length when AES 128-bit encryption algorithm is used. It is recommended to create key name and provide the key-string and lifetime.
- The lifetime period (validity period of the key) can be configured, with a duration in seconds, as a validity period between two dates (for example, Jan 01 2016 to Dec 31 2016), or with infinite validity. The key is valid from the time you configure (in HH:MM:SS format). The duration is configured in seconds. The overlapping time must be configured in two keys to avoid traffic loss.
- The keys roll over to the next key within the same key chain by configuring a second key (key 02) in the key chain and configuring lifetime for the first key. When the lifetime of the first key (key 01) expires,

it automatically rolls over to the next key in the list. If the same key is configured simultaneously on both sides of the link, the key rollover is hitless and the key rolls over without interruption in traffic. Based on IEEE 802.1x, the overlapping time between the keys in a key chain can be up to 20 seconds. The re-key operation can take up to 16 seconds.

Configure MACsec Key Chain

configure

key chain *key-chain-name* **macsec**

key *key-name*

key-string *password* **cryptographic-algorithm** {**aes-256-cmac** | **aes-128-cmac**}

lifetime *start_time start_date* { *end_time end_date* | **duration** *validity* | **infinite** }

exit

commit

Examples

The following is a sample in which the key chain is configured with AES 256-bit encryption algorithm and specific duration for the lifetime period.

```
configure
key chain mac_chain macsec
key 1234abcd5678
key-string 12345678123456781234567812345678123456781234567812345678123456781234567812345678
cryptographic-algorithm aes-256-cmac
lifetime 05:00:00 01 july 2016 duration 1800
exit
commit
```

The following is a sample in which the key chain is configured with AES 256-bit encryption algorithm and defined period for the lifetime period.

```
configure
key chain mac_chain macsec
key 1234abcd5678
key-string 12345678123456781234567812345678123456781234567812345678123456781234567812345678
cryptographic-algorithm aes-256-cmac
lifetime 05:00:00 20 july 2016 12:00:00 30 september 2016
exit
commit
```

The following is a sample in which the key chain is configured with AES 256-bit encryption algorithm and infinite duration for the lifetime period.

```
configure
key chain mac_chain macsec
key 1234abcd5678
key-string 12345678123456781234567812345678123456781234567812345678123456781234567812345678
cryptographic-algorithm aes-256-cmac
lifetime 05:00:00 01 January 2015 infinite
```

```
exit
commit
```

The following is a sample in which the key chain is configured with AES 128-bit encryption algorithm and specific duration for the lifetime period.

```
configure
key chain mac_chain macsec
key abc1
key-string 12345678123456781234567812345678 cryptographic-algorithm aes-128-cmac
lifetime 17:30:00 31 August 2016 duration 4000
exit
commit
```

The following is a sample in which the key chain is configured with AES 128-bit encryption algorithm and defined period for the lifetime period.

```
configure
key chain mac_chain macsec
key abc2
key-string 12345678123456781234567812345678 cryptographic-algorithm aes-128-cmac
lifetime 17:30:00 31 August 2016 12:00:00 30 september 2016
exit
commit
```

The following is a sample in which the key chain is configured with AES 128-bit encryption algorithm and infinite duration for the lifetime period.

```
configure
key chain mac_chain macsec
key abc3
key-string 12345678123456781234567812345678 cryptographic-algorithm aes-128-cmac
lifetime 05:00:00 01 January 2015 infinite
exit
commit
```

Associated Commands

- key chain
- key
- key-string
- cryptographic-algorithm
- lifetime

Verify MACsec Key Chain

show key chain

```
Wed Aug 17 14:34:00.056 IST

Key-chain: TESTMA -(MacSec)

  Key BDA123
```

```
    Key-String -- 08701E1D5D4C53404A5A5E577E7E727F6B647040534355560E080A00005B554F4E
    Cryptographic-Algorithm -- ALG_AES_256_CMAC
    Send lifetime --  19:05:00, 16 Aug 2016 - Always valid  [Valid now]

Key-chain: mac_chain -(MacSec)

  Key abc1
    Key-String -- 12485744465E5A53727A767B676074445F475152020C0E040C5F514B420C0E000B
    Cryptographic-Algorithm -- ALG_AES_128_CMAC
    Send lifetime --  17:30:00, 31 Aug 2016 - (Duration) 4000

  Key abc2
    Key-String -- 135445415F59527D73757A60617745504E5253050D0D050356524A450D0D01040A
    Cryptographic-Algorithm -- ALG_AES_128_CMAC
    Send lifetime --  17:30:00, 31 Aug 2016 - 12:00:00, 30 Sep 2016

  Key abc3
    Key-String -- 101F5B4A5142445C54557878707D65627A4255455754000E0002065D574D400E00
    Cryptographic-Algorithm -- ALG_AES_128_CMAC
    Send lifetime --  05:00:00, 01 Jan 2015 - Always valid  [Valid now]
```

MACsec Policy

You apply a defined MACsec policy to enable MKA on the controller. You can configure these parameters for MACsec policy:

- Policy name, not to exceed 16 ASCII characters.
- Confidentiality (encryption) offset of 0 bytes.
- Replay protection. You can configure MACsec window size, as defined by the number of out-of-order frames that are accepted. This value is used while installing the security associations in the MACsec. A value of 0 means that frames are accepted only in the correct order.
- The cipher suite to be used for MACsec encryption is GCM-AES-XPN-256.
- The range of **key server priority** parameter is 0 to 255. Lower the value, higher the preference to be selected as the key server.
- The **security-policy** parameter configures the type of traffic (encrypted traffic or all traffic) that is allowed through the controller configured with MACsec. The default value of **security-policy** parameter is **must-secure** that indicates unencrypted packets cannot be transmitted or received except MKA control protocol packets.

Configure MACsec Policy

configure

macsec-policy *policy-name*

cipher-suite *encryption-suite*

conf-offset *offset-value*

key-server-priority *value*

security-policy {should-secure | must-secure}

window-size *value*

exit

commit

Examples

Example 1: The following is a sample of configuring the MACsec policy.

```
configure
macsec-policy mac_policy
cipher-suite GCM-AES-XPN-256
conf-offset CONF-OFFSET-0
key-server-priority 0
security-policy must-secure
window-size 64
exit
commit
```

Example 2: If a specific setting does not apply to NCS 1002, the setting is rejected during commit.

```
configure
macsec-policy mac_policy
vlan-tags-in-clear 1
commit


Thu Aug 4 19:31:38.033 UTC

% Failed to commit one or more configuration items during a pseudo-atomic operation. All
changes made have been reverted. Please issue
 'show configuration failed [inheritance]' from this session to view the errors

show configuration failed


Thu Aug 4 19:31:56.601 UTC
!! SEMANTIC ERRORS: This configuration was rejected by
!! the system due to semantic errors. The individual
!! errors with each failed configuration command can be
!! found below.


macsec-policy mac_policy
!!% A verifier or EDM callback function returned: 'not supported': vlan_tags_in_clear is
not supported.

vlan-tags-in-clear 1
!!% A verifier or EDM callback function returned: 'not supported': vlan_tags_in_clear is
not supported.

!
end
```

Example 3: If a specific configuration in the batch operation is not supported, the entire batch is rejected during commit.

```
configure
macsec-policy mac_policy
cipher-suite GCM-AES-XPN-256
window-size 64
```

```
conf-offset CONF-OFFSET-0
commit


Thu Aug 4 19:37:22.355 UTC

% Failed to commit one or more configuration items during a pseudo-atomic operation. All
changes made have been reverted. Please issue 'show configuration failed [inheritance]'
from this session to view the errors

show configuration failed


Thu Aug 4 19:38:29.948 UTC
!! SEMANTIC ERRORS: This configuration was rejected by
!! the system due to semantic errors. The individual
!! errors with each failed configuration command can be
!! found below.


macsec-policy mac_policy
!!% A verifier or EDM callback function returned: 'not supported': The only supported
conf_offset is CONF-OFFSET-0

conf-offset CONF-OFFSET-0
!!% A verifier or EDM callback function returned: 'not supported': The only supported
conf_offset is CONF-OFFSET-0

window-size 64
!!% A verifier or EDM callback function returned: 'not supported': The only supported
conf_offset is CONF-OFFSET-0

cipher-suite GCM-AES-XPN-256
!!% A verifier or EDM callback function returned: 'not supported': The only supported
conf_offset is CONF-OFFSET-0

!
end
```

Associated Commands

- macsec-policy
- cipher-suite
- conf-offset
- key-server-priority
- security-policy
- window-size

Verify MACsec Policy

show macsec policy

```
Sun Dec 18 14:22:23.587 IST

Total Number of Policies = 3
```

```
=================================================================
Policy            Cipher              Key-Svr   Window    Conf
name              Suite               Priority  Size      Offset
=================================================================
*DEFAULT POLICY*  GCM-AES-XPN-256     16        64        0
kcp1              GCM-AES-XPN-256     16        128       0
kcp2              GCM-AES-XPN-256     16        256       0
```

show macsec policy 5

```
Wed Mar 30 12:49:29.371 UTC
=================================================================
Policy            Cipher              Key-Svr   Window    Conf
name              Suite               Priority  Size      Offset
=================================================================
5                 GCM-AES-XPN-256     37        64        0
```

If the values you see are different from the ones you configured, then check your configuration by running the **show run macsec-policy** command.

MACsec Controllers

MACsec controllers are created when a slice is provisioned with the **encrypted** keyword. The MACsec controller is used to configure the MACsec parameters. All the MACsec statistics is available on the MACsec controller. The MACsec controller is represented in the *Rack/Slot/Instance/Port* format, for example, 0/0/0/3.

A unique MAC address is generated for each MACsec controller. When software is upgraded to R6.2.2 with traffic, traffic loss occurs for the slice configured in encrypted mode.

Configure the Slice

You can configure the slice with traffic on client and trunk ports. All five client ports of the slice need to be configured at the same bitrate except for mixed mode configuration. Both the trunk ports are always set with the same FEC mode. The slice can be configured to send encrypted traffic from R6.1.1.

See the Supported Configurations in Encrypted Mode, on page 38 section to determine the supported configurations on the client and trunk ports in each slice configured in encrypted mode

Note When the slice is configured in encrypted mode, the drop-lldp cannot be enabled.

Note When NCS 1002 is installed in a system where both the trunk interfaces in a slice are used, the two 250Gb 16QAM signals need to be co-routed on the same fiber (mandatory when the 5x100Gb client port is provisioned). Also, it is recommended to use adjacent wavelengths when the line modulation is set to 250Gb 16QAM. The reason for this is that the chromatic dispersion generates skew between wavelengths. Assuming a Dispersion of 10000 ps/nm, a span of 500 km, and using adjacent channel, the skew is evaluated in less than 200 ns and it is compensated by the deskew capability of NCS 1002. If the delta between the used channels is increased, the skew increases and it might exceed the skew compensation done by NCS 1002.

To configure the slice with unencrypted traffic, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate** { **10G** | **40G** | **100G** } **trunk bitrate** { **100G** | **200G** | **250G** } **fec** { **softdecision7** | **softdecision20** }

commit

To configure the slice with mixed mode, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate 10G-100G trunk bitrate 200G fec** { **softdecision7** | **softdecision20** }

commit

To configure the slice with encrypted traffic, use the following commands.

configure

hw-module location *location* **slice** [*slice_number* | **all**] **client bitrate** { **10G** | **40G** | **100G** } **trunk bitrate** { **100G** | **200G** } **fec** { **softdecision7** | **softdecision20** } [**encrypted**]

commit

Examples

The following is a sample in which slice 0 is configured in mixed mode, and FEC on the trunk ports is set to softdecision7.

```
configure
hw-module location 0/RP0/CPU0 slice 0 client bitrate 10G-100G trunk bitrate 200G fec
SoftDecision7
commit
```

The following is a sample in which slice 0 is configured to send encrypted traffic with 100G client rate, 200G trunk rate, and FEC on the trunk ports is set to softdecision7.

```
configure
hw-module location 0/RP0/CPU0 slice 0 client bitrate 100G trunk bitrate 200G softdecision7
 encrypted
commit
```

The following is a sample in which slice 0 is configured to send encrypted traffic with 10G client rate, 100G trunk rate, and FEC on the trunk ports is set to softdecision20. When a slice is configured with 10G client rate in encrypted mode, ten MACsec controllers are created for each slice. When all the four slices are configured with 10G client rate in encrypted mode, forty MACsec controllers are created for NCS 1002. Two MACsec controllers are created for the middle port, four controllers for the fourth port, and four controllers for the fifth port per slice.

```
configure
hw-module location 0/RP0/CPU0 slice 0 client bitrate 10G trunk bitrate 100G softdecision20
 encrypted
commit
```

The following is a sample in which slice 0 is configured to send encrypted traffic with 40G client rate, 100G trunk rate, and FEC on the trunk ports is set to softdecision20.

```
configure
hw-module location 0/RP0/CPU0 slice 0 client bitrate 40G trunk bitrate 100G softdecision20
 encrypted
commit
```

The following is a sample to configure all the slices with a specific client rate and trunk rate.

```
configure
hw-module location 0/RP0/CPU0 slice all client bitrate 10G trunk bitrate 100G fec
softDecision7
commit
```

```
configure
hw-module location 0/RP0/CPU0 slice all client bitrate 40G trunk bitrate 100G fec
softDecision7
commit
```

```
configure
hw-module location 0/RP0/CPU0 slice all client bitrate 100G trunk bitrate 200G fec
softDecision7
commit
```

The following is a sample to remove the configuration from all the slices.

```
configure
no hw-module location 0/RP0/CPU0 slice all client bitrate 10G trunk bitrate 100G fec
softDecision7
commit
```

```
configure
no hw-module location 0/RP0/CPU0 slice all client bitrate 40G trunk bitrate 100G fec
softDecision7
commit
```

```
configure
no hw-module location 0/RP0/CPU0 slice all client bitrate 100G trunk bitrate 200G fec
softDecision7
commit
```

Associated Commands

- hw-module
- show hw-module

Verify Slice Configuration

Use this procedure to verify whether the slice is correctly configured.

show hw-module { **slice** [*slicenumber* | **all**] }

Example:

```
RP/0/RP0/CPU0:ios# show hw-module slice 0
```

```
Thu Aug 11 16:16:58.935 IST
Slice ID:                0
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
LLDP Drop Enabled:       FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/6
Traffic Split Percentage

HundredGigECtrlr0/0/0/3                  100
HundredGigECtrlr0/0/0/4                  100
```

```
RP/0/RP0/CPU0:ios# show hw-module slice 0


Sun Dec 18 13:59:18.805 IST
Slice ID:                0
Status:                  Provisioned
Client Bitrate:          40
Trunk Bitrate:           100
DP FPGA FW Type:         MM40
DP FPGA FW Version:      03.00
HW Status:               CURRENT

Encryption Supported:    TRUE
LLDP Drop Enabled:       FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/6
Traffic Split Percentage

FortyGigECtrlr0/0/0/3                    100
FortyGigECtrlr0/0/0/4                    100
```

```
RP/0/RP0/CPU0:ios# show hw-module slice 1


Tue Jan  1 06:55:12.293 UTC
Slice ID:                1
Status:                  Provisioned
Client Bitrate:          10
Trunk Bitrate:           100
DP FPGA FW Type:         MM10
DP FPGA FW Version:      03.00
HW Status:               CURRENT

Encryption Supported:    TRUE
LLDP Drop Enabled:       FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/13
Traffic Split Percentage

TenGigECtrlr0/0/0/9/1                            100
TenGigECtrlr0/0/0/9/2                            100
TenGigECtrlr0/0/0/10/1                           100
TenGigECtrlr0/0/0/10/2                           100
TenGigECtrlr0/0/0/10/3                           100
TenGigECtrlr0/0/0/10/4                           100
TenGigECtrlr0/0/0/11/1                           100
TenGigECtrlr0/0/0/11/2                           100
TenGigECtrlr0/0/0/11/3                           100
TenGigECtrlr0/0/0/11/4                           100
```

```
RP/0/RP0/CPU0:ios# show hw-module slice 2


Slice ID:               2
Status:                 Provisioned
Client Bitrate:         10,100
Trunk Bitrate:          200
DP FPGA FW Type:        RMM
DP FPGA FW Version:     04.00
HW Status:              CURRENT

Encryption Supported:   FALSE
LLDP Drop Enabled:      FALSE
Client Port -   Trunk Port          CoherentDSP0/0/0/19  CoherentDSP0/0/0/20
Traffic Split Percentage

HundredGigECtrlr0/0/0/14                        100                   0
HundredGigECtrlr0/0/0/15                        100                   0
HundredGigECtrlr0/0/0/16                          0                 100
TenGigECtrlr0/0/0/17/1                            0                 100
TenGigECtrlr0/0/0/17/2                            0                 100
TenGigECtrlr0/0/0/17/3                            0                 100
TenGigECtrlr0/0/0/17/4                            0                 100
TenGigECtrlr0/0/0/18/1                            0                 100
TenGigECtrlr0/0/0/18/2                            0                 100
TenGigECtrlr0/0/0/18/3                            0                 100
TenGigECtrlr0/0/0/18/4                            0                 100
```

Displays the details of the slice such as the slice ID, client rate, trunk rate, and the traffic percentage carried on the trunk ports. The **Encryption Supported** field indicates whether the slice is provisioned with firmware that supports encryption or not.

Note The HW Status field might display "Need Upgrade" when the user needs to use the MACsec feature and upgrades from R6.0.1 to 6.1.1. Hence, the control FPGA (CTRL_BKP_UP, CTRL_BKP_LOW, CTRL_FPGA_UP, and CTRL_FPGA_LOW) needs to be upgraded to the latest firmware version provided by R6.1.1. See Verify Firmware Version for more information.

The Provisioned status does not indicate that the traffic can flow immediately. For example, use the **show controllers maCSecCtrlr 0/0/0/3** command output to view the provisioning information of the port after the slice is provisioned.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module slice all


Thu Aug 11 16:16:58.935 IST
Slice ID:               0
Status:                 Provisioned
Client Bitrate:         100
Trunk Bitrate:          200
DP FPGA FW Type:        M100
DP FPGA FW Version:     02.00
HW Status:              CURRENT

Encryption Supported:   TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/6
Traffic Split Percentage

HundredGigECtrlr0/0/0/3                   100
HundredGigECtrlr0/0/0/4                   100

Slice ID:               1
Status:                 Provisioned
Client Bitrate:         100
```

```
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/13
Traffic Split Percentage

HundredGigECtrlr0/0/0/10                    100
HundredGigECtrlr0/0/0/11                    100

Slice ID:                2
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/20
Traffic Split Percentage

HundredGigECtrlr0/0/0/17                   100
HundredGigECtrlr0/0/0/18                   100

Slice ID:                3
Status:                  Provisioned
Client Bitrate:          100
Trunk Bitrate:           200
DP FPGA FW Type:         M100
DP FPGA FW Version:      02.00
HW Status:               CURRENT

Encryption Supported:    TRUE
Client Port -   Trunk Port          CoherentDSP0/0/0/27
Traffic Split Percentage

HundredGigECtrlr0/0/0/24                   100
HundredGigECtrlr0/0/0/25                   100
```

Associated Commands

- hw-module
- show hw-module

Apply MACsec Configuration on MACsec Controller

You can apply the MACsec key chain and policy configuration on the MACsec controller.

configure

controller MACSecCtrl *Rack/Slot/Instance/Port*

macsec psk-keychain *key-chain-name* [**policy** *policy-name*]

exit

commit

Example

```
configure
controller MACSecCtrl 0/0/0/3
macsec psk-keychain mac_chain policy mac_policy
exit
commit
```

Associated Commands

- controller mACSecCtrlr
- macsec psk-keychain

Verify MACsec Configuration on MACsec Controller

1. Verify the MACsec configuration on the controller.

   show macsec mka summary

   ```
   Wed Mar 30 13:35:15.497 UTC
   NODE: node0_RP0_CPU0
   ============================================================
    Interface       Status          Cipher-Suite         KeyChain
   ============================================================
    MS0/0/0/03       Secured         GCM-AES-XPN-256     mac_chain

   Total MACSec Sessions : 1
        Secured Sessions : 1
        Pending Sessions : 0
   ```

   The **Status** field in the output confirms that the respective controller is **Secured**. If MACsec encryption is not successfully configured, you will see a status such as **Pending** or **Init**.

2. Verify whether the MKA session is secured with MACsec on the respective controller.

   show macsec mka session

   ```
   Sun Dec 18 14:20:50.626 IST
   NODE: node0_RP0_CPU0
   ================================================================================
         Interface          Local-TxSCI        # Peers    Status  Key-Server
   ================================================================================
        MS0/0/0/3       3820.563b.eacc/0003       1      Secured     YES
        MS0/0/0/18       3820.563b.eacc/0012      1      Secured     NO
        MS0/0/0/17       3820.563b.eacc/0011      1      Secured     NO
        MS0/0/0/4       3820.563b.eacc/0004       1      Secured     YES
   ```

   show macsec mka session controller MS0/0/0/03 detail

   ```
   Tue Aug 16 14:08:04.927 IST

   MKA Detailed Status for MKA Session
   ===================================
   Status: SECURED - Secured MKA Session with MACsec
   ```

```
Local Tx-SCI            : 3820.563b.eacc/0003
Local Tx-SSCI           : 2
Interface MAC Address   : 3820.563b.eacc
MKA Port Identifier     : 10
Interface Name          : MS0/0/0/03
CAK Name (CKN)         : ABC1000000000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)  : 6609E2B5F8ACC8653301503B
Message Number (MN)     : 39
Authenticator           : NO
Key Server              : YES
MKA Cipher Suite        : AES-128-CMAC

Latest SAK Status       : Rx & Tx
Latest SAK AN           : 0
Latest SAK KI (KN)      : 6609E2B5F8ACC8653301503B00000001 (1)
Old SAK Status          : FIRST-SAK
Old SAK AN              : 0
Old SAK KI (KN)         : FIRST-SAK (0)

SAK Transmit Wait Time  : 0s (Not waiting for any peers to respond)
SAK Retire Time         : 0s (No Old SAK to retire)

MKA Policy Name         : *DEFAULT POLICY*
Key Server Priority     : 16
Replay Window Size      : 64
Confidentiality Offset  : 0
Algorithm Agility       : 80C201
SAK Cipher Suite        : 0080C20001000004 (GCM-AES-XPN-256)
MACsec Capability       : 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired          : YES

# of MACsec Capable Live Peers           : 1
# of MACsec Capable Live Peers Responded : 1

Live Peer List:
  MI                       MN          Rx-SCI (Peer)        SSCI KS-Priority
  -----------------------------------------------------------------------------
  389DF014D752B8065B548283  62         3820.563b.eacc/0012     1     16

Potential Peer List:
  MI                       MN          Rx-SCI (Peer)        SSCI KS-Priority
  -----------------------------------------------------------------------------
```

The **Status** field in the output verifies if the MKA session is secured with MACsec encryption. The output also displays information about the controller and other MACsec parameters.

3. Verify the MACsec session counter statistics.

   show macsec mka statistics location 0/RP0/CPU0

```
Thu Aug 11 16:02:41.330 IST

MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 0
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
```

```
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated............. 0
   SAKs Rekeyed............... 0
   SAKs Received.............. 0
   SAK Responses Received..... 0

MKPDU Statistics
   MKPDUs Validated & Rx...... 5
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 4
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0

MKPDU Failures
   MKPDU Tx......................... 0
   MKPDU Rx Validation.............. 0
   MKPDU Rx Bad Peer MN............. 0
   MKPDU Rx Non-recent Peerlist MN.. 0
   MKPDU Rx Drop SAKUSE, KN mismatch...... 0
   MKPDU Rx Drop SAKUSE, Rx Not Set....... 0
   MKPDU Rx Drop SAKUSE, Key MI mismatch.. 0
   MKPDU Rx Drop SAKUSE, AN Not in Use.... 0
   MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set. 0

IOX Global Statistics
   MKPDUs Rx IDB not found.... 0
   MKPDUs Rx Invalid CKN...... 0
   MKPDUs Tx Invalid IDB...... 0
   MKPDUs Tx Pkt Build Fail... 0
```

The counters display the MACsec PDUs transmitted, validated, and received. The output also displays transmission errors, if any. This completes the verification of MACsec encryption on NCS 1002.

a. Verify the status of the MACsec controller.

show macsec platform status controller MacSecCtrlr 0/0/0/3

```
Mon Jun  6 20:57:15.900 UTC

-------------------------------------

Interface Status

-------------------------------------
    ReplayWindowSize       :  64
    MustSecure             :  TRUE
    SecureMode             :  2

-------------------------------------

Encrypted Secure Channel Status

-------------------------------------
    ProtectionEnabled      :  TRUE
    SecureChannelID        :  0x0200d05a57395540
    ConfidentialityOffset  :  0
    CipherSuite            :  GCM-AES-XPN-256
    SecureTagLength        :  16
    InitialPacketNumber    :  1
    MaxPacketNumber        :  18446744073709551615
    RecentPacketNumber     :  364865080

-------------------------------------

Encrypted Active Associations

-------------------------------------
    AssociationNumber      :  1
    DeviceAssociationNum   :  1
    ShortSecureChannelID   :  1
    ProgrammedTime         :  2016 Jun 6 20:57:09.690
    KeyCRC                 :  0x6fe6f59c
    XpnSalt                :  0xffca89c5 0x4a307f93 0xd3df482e


-------------------------------------

Decrypted Secure Channel Status

-------------------------------------
    ProtectionEnabled      :  TRUE
    SecureChannelID        :  0x0100d05a57395540
    ConfidentialityOffset  :  0
    CipherSuite            :  GCM-AES-XPN-256
    InitialPacketNumber    :  1
    MaxPacketNumber        :  18446744073709551615
    RecentPacketNumber     :  370010268

-------------------------------------

Decrypted Active Associations

-------------------------------------
```

```
AssociationNumber      :  1
DeviceAssociationNum   :  1
ShortSecureChannelID   :  2
ProgrammedTime         :  2016 Jun 6 20:57:09.550
KeyCRC                 :  0x6fe6f59c
XpnSalt                :  0xfcca89c5 0x4a307f93 0xd3df482e
```

When IOS XR is reloaded, two association numbers are displayed under Decrypted Active Associations. After the reload, key roll over is required. When the key rollover happens, the active association number is associated.

Verify State of MACSec Controller

The state of MACSec controller can be verified using the **show controllers MACSecCtrlr** *R/S/I/P* command. If the state of MACSec controller is down, the corresponding MKA sessions do not come up.

The state of MACSec controller is down upon one of the following conditions.

- State of the corresponding Ethernet controller is Admin Down. The state can be verified using the **show controllers HundredGigECtrlr** *R/S/I/P* command.
- State of the optics controller is Admin Down or Operational Down. The state can be verified using the **show controllers optics** *R/S/I/P* command.
- Client optics is not present. The client optics can be verified using the **show inventory** command.

The state of the Ethernet controller can be changed from Admin Down using the following commands.

```
configure
controller HundredGigECtrlr Rack/Slot/Instance/Port
no shutdown
commit
```

The state of the optics controller can be changed from Admin Down or Operational Down using the following commands.

```
configure
controller optics Rack/Slot/Instance/Port
no shutdown
commit
```

SecY Statistics

SecY statistics is used to identify issues with the encrypted traffic.

Before You Begin

Ensure that MKA sessions are established. See Verify MACsec Configuration on MACsec Controller, on page 52 for more information.

100G MACsec

show macsec secy stats controller MACSecCtrlr 0/0/0/3 SC

```
Tue Jan 22 04:42:32.044 IST
Interface Stats
    InPktsUntagged     :  0
    InPktsNoTag        :  0
    InPktsBadTag       :  0
    InPktsUnknownSCI   :  0
    InPktsNoSCI        :  0
    InPktsOverrun      :  0
    InOctetsValidated  :  0
    InOctetsDecrypted  :  121697919056
    OutPktsUntagged    :  0
    OutPktsTooLong     :  0
    OutOctetsProtected :  0
    OutOctetsEncrypted :  194316914428

SC Stats
  TxSC Stats
    OutPktsProtected   : 0
    OutPktsEncrypted   : 130941317
    OutOctetsProtected : 0
    OutOctetsEncrypted : 194316914428
    OutPktsTooLong     : 0
    TxSA Stats
      TxSA 0:
        OutPktsProtected : 0
        OutPktsEncrypted : 0
        NextPN           : 0
      TxSA 1:
        OutPktsProtected : 0
        OutPktsEncrypted : 130941317
        NextPN           : 130940105
      TxSA 2:
        OutPktsProtected : 0
        OutPktsEncrypted : 0
        NextPN           : 0
      TxSA 3:
        OutPktsProtected : 0
        OutPktsEncrypted : 0
        NextPN           : 0

  RxSC Stats
    RxSC 1: 0
      InPktsUnchecked     : 0
      InPktsDelayed       : 0
      InPktsLate          : 0
      InPktsOK            : 82006684
      InPktsInvalid       : 0
      InPktsNotValid      : 0
      InPktsNotUsingSA    : 0
      InPktsUnusedSA      : 0
      InPktsUntaggedHit   : 0
      InOctetsValidated   : 0
      InOctetsDecrypted   : 121697919056
    RxSA Stats
      RxSA 0:
        InPktsUnusedSA      : 0
        InPktsNotUsingSA    : 0
        InPktsNotValid      : 0
        InPktsInvalid       : 0
        InPktsOK            : 0
        NextPN              : 1
      RxSA 1:
        InPktsUnusedSA      : 0
```

```
        InPktsNotUsingSA    : 0
        InPktsNotValid      : 0
        InPktsInvalid       : 0
        InPktsOK            : 82006684
        NextPN              : 82004142
      RxSA 2:
        InPktsUnusedSA      : 0
        InPktsNotUsingSA    : 0
        InPktsNotValid      : 0
        InPktsInvalid       : 0
        InPktsOK            : 0
        NextPN              : 0
      RxSA 3:
        InPktsUnusedSA      : 0
        InPktsNotUsingSA    : 0
        InPktsNotValid      : 0
        InPktsInvalid       : 0
        InPktsOK            : 0
        NextPN              : 0
```

The SecY SA counters are displayed as 64 bit values in the CLI.

10G MACsec

show macsec secy stats controller MACSecCtrlr 0/0/0/3/1 SC

```
Mon Dec 19 17:04:00.467 IST
Interface Stats
    InPktsUntagged     :  0
    InPktsNoTag        :  0
    InPktsBadTag       :  0
    InPktsUnknownSCI   :  0
    InPktsNoSCI        :  0
    InPktsOverrun      :  0
    InOctetsValidated  :  0
    InOctetsDecrypted  :  3244694362816
    OutPktsUntagged    :  0
    OutPktsTooLong     :  0
    OutOctetsProtected :  0
    OutOctetsEncrypted :  3225943872072

SC Stats
  TxSC Stats
    OutPktsProtected   : 0
    OutPktsEncrypted   : 336597056
    OutOctetsProtected : 0
    OutOctetsEncrypted : 3225943872072
    OutPktsTooLong     : 0

 RxSC Stats
    RxSC 1: 0
      InPktsUnchecked     : 0
      InPktsDelayed       : 0
      InPktsLate          : 0
      InPktsOK            : 338553493
      InPktsInvalid       : 0
      InPktsNotValid      : 0
      InPktsNotUsingSA    : 1320396
      InPktsUnusedSA      : 0
      InPktsUntaggedHit   : 0
      InOctetsValidated   : 0
      InOctetsDecrypted   : 3244694362816
```

Trunk Side Statistics

Trunk side statistics is used to isolate issues with the encrypt and decrypt blocks. In the Tx direction, the trunk side Egress statistics display statistics after the encrypt block. In the Rx direction, the trunk side Ingress statistics display statistics before the decrypt block.

show controllers MACSecCtrlr 0/0/0/3 stats

```
Tue Jan 22 04:51:40.858 IST
Statistics for interface MACSecCtrlr0/0/0/3 (cached values):

Ingress:
    Input total bytes           = 805443936740
    Input good bytes            = 805443936740

    Input total packets         = 525746695
    Input 802.1Q frames         = 0
    Input pause frames          = 0
    Input pkts 64 bytes         = 0
    Input pkts 65-127 bytes     = 0
    Input pkts 128-255 bytes    = 0
    Input pkts 256-511 bytes    = 0
    Input pkts 512-1023 bytes   = 0
    Input pkts 1024-1518 bytes  = 0
    Input pkts 1519-Max bytes   = 0

    Input good pkts             = 525746695
    Input unicast pkts          = 0
    Input multicast pkts        = 0
    Input broadcast pkts        = 0

    Input drop overrun          = 0
    Input drop abort            = 0
    Input drop invalid VLAN     = 0
    Input drop invalid DMAC     = 0
    Input drop invalid encap    = 0
    Input drop other            = 0

    Input error giant           = 0
    Input error runt            = 0
    Input error jabbers         = 0
    Input error fragments       = 0
    Input error CRC             = 0
    Input error collisions      = 0
    Input error symbol          = 0
    Input error other           = 0

    Input MIB giant             = 0
    Input MIB jabber            = 0
    Input MIB CRC               = 0

Egress:
    Output total bytes          = 880411742408
    Output good bytes           = 880411742408

    Output total packets        = 574681294
    Output 802.1Q frames        = 0
    Output pause frames         = 0
    Output pkts 64 bytes        = 0
    Output pkts 65-127 bytes    = 0
```

```
    Output pkts 128-255 bytes   = 0
    Output pkts 256-511 bytes   = 0
    Output pkts 512-1023 bytes  = 0
    Output pkts 1024-1518 bytes = 0
    Output pkts 1519-Max bytes  = 0

    Output good pkts            = 574681294
    Output unicast pkts         = 0
    Output multicast pkts       = 0
    Output broadcast pkts       = 0

    Output drop underrun        = 0
    Output drop abort           = 0
    Output drop other           = 0

    Output error other          = 0
```

clear controller MACSecCtrlr 0/0/0/3 stats

```
Tue Jan 22 04:52:40.858 IST
```

show controllers macSecCtrlr 0/0/0/3 stats | inc total

```
Tue Jan 22 04:51:45.227 IST
    Input total bytes           = 805443936740
    Input total packets         = 525746695
    Output total bytes          = 880411742408
    Output total packets        = 574681294
RP/0/RP0/CPU0:ios#show controllers macSecCtrlr 0/0/0/3 stats | inc total
Tue Jan 22 04:51:47.695 IST
    Input total bytes           = 805443936740
    Input total packets         = 525746695
```

Control Plane Statistics

show macsec mka statistics controller macSecCtrlr 0/0/0/3

This command displays control plane statistics for the specific MACSec controller.

```
Tue Jan 22 04:57:57.450 IST


MKA Statistics for Session on interface (MS0/0/0/3)
=======================================================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated.......... 1
   SAKs Rekeyed............ 0
   SAKs Received........... 0
   SAK Responses Received.. 1

MKPDU Statistics
   MKPDUs Transmitted...... 3305
      "Distributed SAK".. 1
```

```
      "Distributed CAK".. 0
   MKPDUs Validated & Rx... 3305
      "Distributed SAK".. 0
      "Distributed CAK".. 0

MKA IDB Statistics
   MKPDUs Tx Success.......... 3305
   MKPDUs Tx Fail............. 0
   MKPDUS Tx Pkt build fail... 0
   MKPDUS No Tx on intf down.. 2
   MKPDUS No Rx on intf down.. 0
   MKPDUs Rx CA Not found..... 0
   MKPDUs Rx Error............ 0
   MKPDUs Rx Success.......... 3305
   MKPDUs Rx Invalid Length... 0
   MKPDUs Rx Invalid CKN...... 0

MKPDU Failures
   MKPDU Rx Validation (ICV).................. 0
   MKPDU Rx Bad Peer MN....................... 0
   MKPDU Rx Non-recent Peerlist MN............ 0
   MKPDU Rx Drop SAKUSE, KN mismatch......... 0
   MKPDU Rx Drop SAKUSE, Rx Not Set.......... 0
   MKPDU Rx Drop SAKUSE, Key MI mismatch..... 0
   MKPDU Rx Drop SAKUSE, AN Not in Use....... 0
   MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set.... 0
   MKPDU Rx Drop Packet, Ethertype Mismatch.. 0
   MKPDU Rx Drop Packet, Source MAC NULL..... 0
   MKPDU Rx Drop Packet, Destination MAC NULL 0
   MKPDU Rx Drop Packet, Payload NULL........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0

CA Failures
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0
```

clear macsec mka statistics controller macSecCtrlr 0/0/0/3

This command clears control plane statistics for the specific MACSec controller.

```
Tue Jan 22 04:59:33.830 IST
```

Configuring MACsec Threshold Crossing Alerts

You can configure MACsec Threshold Crossing Alerts (TCA) at mac-sec ether, secy-if (interface), and secy-tx. There is no default threshold, mimimum or maximum threshold for configuring MACsec TCA. You can configure it between the range 1 to 4294967295. By default, you can find TCA in **show logging** command. You can configure syslog server in MACsec TCA, and view TCA in syslog server such as EPNM speicific

parameter. You can set TCA for all supported buckets such as 0-sec/15-mins/24-hour for parameters in mac-sec ether/ secy-if/ secy-tx, secy-rx.

Use the following command to configure the MACsec Threshold Crossing Alerts (TCA) at MACsec ether layer, MACsec-secy-if, MACsec-secy-Tx, and /or MACsec-secy-Rx:

controllers macSecCtrlr *R/S/P* {**pm** {**30 sec** | **15-min** | **24-hour**} {**macsec-ether** | **macsec-secy-if** | **macsec-secy-tx** | **macsec-secy-rx**} {**report** | **threshold** {**in-oct-decrypted** | **out-oct-decrypted**} *value*} **enable**

Examples

The following is a sample to configure the MACsec TCA parameters for rx-pkt at macsec-ether level for MACsec controller in 15 min intervals:

```
controllers macSecCtrlr 0/0/0/11/1
 pm 15-min macsec-ether report rx-pkt enable
pm 15-min macsec-ether threshold rx-pkt 1000000
```

The following is a sample to configure the MACsec TCA parameters for rx-util at macsec-ether level for MACsec controller in 15 min intervals:

```
controllers macSecCtrlr 0/0/0/11/1
pm 15-min macsec-ether report rx-util enable
pm 15-min macsec-ether threshold rx-util 10
```

The following is a sample to configure the MACsec TCA parameters for out-octets at macsec-ether level for MACsec controller in 15 min intervals:

```
controllers macSecCtrlr 0/0/0/11/1
pm 15-min macsec-ether report out-octets enable
pm 15-min macsec-ether threshold out-octets 100000
```

The following is a sample to configure the MACsec TCA parameters for rx-pkt at MAC-SECy-If controller in 30 sec interval:

```
controller MACSecCtrlr0/0/0/4
pm 15-min macsec-ether report rx-pkt enable
pm 15-min macsec-ether threshold rx-pkt 1000
```

Clear Commands

You can use the following commands to clear the PMs across different buckets:

```
clear controller macSecCtrlr 0/0/0/10 pm 15-min
clear controller macSecCtrlr 0/0/0/10 pm 30-sec
clear controller macSecCtrlr 0/0/0/10 pm 24-hour
```

View MACsec PM Parameters

You must configure MACSec controllers to view MACsec performance. To configure MACSec controllers , seeApply MACsec Configuration on MACsec Controller, on page 51.

Use the following commands to view the MACsec performance monitoring at MACsec ether layer, MACsec-secy-if, MACsec-secy-Tx, and /or MACsec-secy-Rx:

show controllers macSecCtrlr *R/S/P*{ **pm**{**current** |**history**} { **30 sec** |**15-min** | **24-hour** } {**macsec-ether** | **macsec-secy-if** | **macsec-secy-tx** | **macsec-secy-rx**}

```
RP/0/RP0/CPU0:ios#show controllers macSecCtrlr 0/0/0/9/1 pm current 30-sec macsec-ether
```

Displays the current performance monitoring parameters of the Ethernet controller in 30 second interval.

```
ETHER in the current interval [23:10:30 - 23:10:31 Sat Mar 18 2017]

ETHER current bucket type : Valid
 RX-UTIL[%]                : 92.75      Threshold : 0.00      TCA(enable) : NO
 TX-UTIL[%]                : 82.26      Threshold : 0.00      TCA(enable) : NO
 RX-PKT                    : 1077504     Threshold : 0         TCA(enable) : NO
 STAT-PKT                  : 0           Threshold : 0         TCA(enable) : NO
 OCTET-STAT                : 1137844152  Threshold : 0         TCA(enable) : NO
 OVERSIZE-PKT              : 0           Threshold : 0         TCA(enable) : NO
 FCS-ERR                   : 0           Threshold : 0          TCA(enable) : NO
 LONG-FRAME                : 0           Threshold : 0          TCA(enable) : NO
 JABBER-STATS              : 0           Threshold : 0          TCA(enable) : NO
 64-OCTET                  : 0           Threshold : 0          TCA(enable) : NO
 65-127-OCTET              : 0           Threshold : 0           TCA(enable) : NO
 128-255-OCTET             : 0           Threshold : 0           TCA(enable) : NO
 256-511-OCTET             : 0           Threshold : 0           TCA(enable) : NO
 512-1023-OCTET            : 0           Threshold : 0           TCA(enable) : NO
 1024-1518-OCTET           : 0           Threshold : 0           TCA(enable) : NO
 IN-UCAST                  : 0           Threshold : 0           TCA(enable) : NO
 IN-MCAST                  : 0           Threshold : 0           TCA(enable) : NO
 IN-BCAST                  : 0           Threshold : 0           TCA(enable) : NO
 OUT-UCAST                 : 0           Threshold : 0           TCA(enable) : NO
 OUT-BCAST                 : 0            Threshold : 0          TCA(enable) : NO
 OUT-MCAST                 : 0            Threshold : 0          TCA(enable) : NO
 TX-PKT                    : 955636       Threshold : 0          TCA(enable) : NO
 OUT-OCTET                 : 1009150716   Threshold : 2000       TCA(enable) : NO
 IFIN-ERRORS               : 0            Threshold : 0          TCA(enable) : NO
 IFIN-OCTETS               : 0            Threshold : 0          TCA(enable) : NO
 STAT-MULTICAST-PKT        : 0            Threshold : 0          TCA(enable) : NO
 STAT-BROADCAST-PKT        : 0            Threshold : 0          TCA(enable) : NO
 STAT-UNDERSIZED-PKT       : 0            Threshold : 0          TCA(enable) : NO
 IN_GOOD_BYTES             : 0            Threshold : 0          TCA(enable) : NO
 IN_GOOD_PKTS              : 0            Threshold : 0          TCA(enable) : NO
 IN_DROP_OTHER             : 0            Threshold : 0          TCA(enable) : NO
 IN_ERROR_FRAGMENTS        : 0            Threshold : 0          TCA(enable) : NO
 IN_PKT_64_OCTET           : 0            Threshold : 0          TCA(enable) : NO
 IN_PKTS_65_127_OCTETS     : 0            Threshold : 0          TCA(enable) : NO
 IN_PKTS_128_255_OCTETS    : 0            Threshold : 0          TCA(enable) : NO
 IN_PKTS_256_511_OCTETS    : 0            Threshold : 0          TCA(enable) : NO
 IN_PKTS_512_1023_OCTETS   : 0            Threshold : 0          TCA(enable) : NO
 IN_PKTS_1024_1518_OCTETS  : 0            Threshold : 0          TCA(enable) : NO
 TX_UNDERSIZED_PKT         : 0            Threshold : 0          TCA(enable) : NO
 TX_OVERSIZED_PKT          : 0            Threshold : 0          TCA(enable) : NO
 TX_FRAGMENTS              : 0            Threshold : 0          TCA(enable) : NO
 TX_JABBER                 : 0            Threshold : 0          TCA(enable) : NO
 TX_BAD_FCS                : 0            Threshold : 0          TCA(enable) : NO
```

Example

```
ios#show controllers macSecCtrlr 0/0/0/9/1 pm current 15-min macsec-ether
```

Displays the current performance monitoring parameters of the Ethernet controller in 15 minute intervals

```
RP/0/RP0/CPU0:ios#show controllers macSecCtrlr 0/0/0/9/1 pm current 15-min macsec-ether
Sat Mar 18 23:10:41.410 IST
ETHER in the current interval [23:00:00 - 23:10:41 Sat Mar 18 2017]
ETHER current bucket type : Valid
 RX-UTIL[%]                : 92.75      Threshold : 0.00      TCA(enable) : NO
 TX-UTIL[%]                : 82.26      Threshold : 0.00      TCA(enable) : NO
```

```
 RX-PKT                    : 690733237           Threshold : 0           TCA(enable) :
NO
 STAT-PKT                  : 0                   Threshold : 0           TCA(enable) :
NO
 OCTET-STAT                : 729414298536        Threshold : 0           TCA(enable) :
NO
 OVERSIZE-PKT              : 0                   Threshold : 0           TCA(enable) :
NO
 FCS-ERR                   : 0                   Threshold : 0           TCA(enable) :
NO
 LONG-FRAME                : 0                   Threshold : 0           TCA(enable) :
NO
 JABBER-STATS              : 0                   Threshold : 0           TCA(enable) :
NO
 64-OCTET                  : 0                   Threshold : 0           TCA(enable) :
NO
 65-127-OCTET              : 0                   Threshold : 0           TCA(enable) :
NO
 128-255-OCTET             : 0                   Threshold : 0           TCA(enable) :
NO
 256-511-OCTET             : 0                   Threshold : 0           TCA(enable) :
NO
 512-1023-OCTET            : 0                   Threshold : 0           TCA(enable) :
NO
 1024-1518-OCTET           : 0                   Threshold : 0           TCA(enable) :
NO
 IN-UCAST                  : 0                   Threshold : 0           TCA(enable) :
NO
 IN-MCAST                  : 0                   Threshold : 0           TCA(enable) :
NO
 IN-BCAST                  : 0                   Threshold : 0           TCA(enable) :
NO
 OUT-UCAST                 : 0                   Threshold : 0           TCA(enable) :
NO
 OUT-BCAST                 : 0                   Threshold : 0           TCA(enable) :
NO
 OUT-MCAST                 : 0                   Threshold : 0           TCA(enable) :
NO
 TX-PKT                    : 612577128           Threshold : 0           TCA(enable) :
NO
 OUT-OCTET                 : 646881447168        Threshold : 8000        TCA(enable) :
NO
 IFIN-ERRORS               : 0                   Threshold : 0           TCA(enable) :
NO
 IFIN-OCTETS               : 0                   Threshold : 0           TCA(enable) :
NO
 STAT-MULTICAST-PKT        : 0                   Threshold : 0           TCA(enable) :
NO
 STAT-BROADCAST-PKT        : 0                   Threshold : 0           TCA(enable) :
NO
 STAT-UNDERSIZED-PKT       : 0                   Threshold : 0           TCA(enable) :
NO
 IN_GOOD_BYTES             : 0                   Threshold : 0           TCA(enable) :
NO
 IN_GOOD_PKTS              : 0                   Threshold : 0           TCA(enable) :
NO
 IN_DROP_OTHER             : 0                   Threshold : 0           TCA(enable) :
NO
 IN_ERROR_FRAGMENTS        : 0                   Threshold : 0           TCA(enable) :
NO
 IN_PKT_64_OCTET           : 0                   Threshold : 0           TCA(enable) :
NO
 IN_PKTS_65_127_OCTETS     : 0                   Threshold : 0           TCA(enable) :
NO
```

```
 IN_PKTS_128_255_OCTETS    : 0                    Threshold : 0            TCA(enable) :
NO
 IN_PKTS_256_511_OCTETS    : 0                    Threshold : 0            TCA(enable) :
NO
 IN_PKTS_512_1023_OCTETS   : 0                    Threshold : 0            TCA(enable) :
NO
 IN_PKTS_1024_1518_OCTETS  : 0                    Threshold : 0            TCA(enable) :
NO
 TX_UNDERSIZED_PKT         : 0                    Threshold : 0            TCA(enable) :
NO
 TX_OVERSIZED_PKT          : 0                    Threshold : 0            TCA(enable) :
NO
 TX_FRAGMENTS              : 0                    Threshold : 0            TCA(enable) :
NO
 TX_JABBER                 : 0                    Threshold : 0            TCA(enable) :
NO
 TX_BAD_FCS                : 0                    Threshold : 0            TCA(enable) :
NO
```

Example

```
ios#show controllers macSecCtrlr 0/0/0/9/1 pm current 24-hour macsec-ether
```

Displays the current performance monitoring parameters of the Ethernet controller in 24 hour intervals.

```
ios#show controllers macSecCtrlr 0/0/0/9/1 pm current 24-hour macsec-ether
Sat Mar 18 23:10:49.939 IST
ETHER in the current interval [00:00:00 - 23:10:50 Sat Mar 18 2017]
ETHER current bucket type : Invalid
 RX-UTIL[%]                : 92.75      Threshold : 0.00      TCA(enable) : NO
 TX-UTIL[%]                : 82.26      Threshold : 0.00      TCA(enable) : NO
 RX-PKT                    : 1508621424           Threshold : 0            TCA(enable) :
NO
 STAT-PKT                  : 0                    Threshold : 0            TCA(enable) :
NO
 OCTET-STAT                : 1593104223188        Threshold : 0            TCA(enable) :
NO
 OVERSIZE-PKT              : 0                    Threshold : 0            TCA(enable) :
NO
 FCS-ERR                   : 0                    Threshold : 0            TCA(enable) :
NO
 LONG-FRAME                : 0                    Threshold : 0            TCA(enable) :
NO
 JABBER-STATS              : 0                    Threshold : 0            TCA(enable) :
NO
 64-OCTET                  : 0                    Threshold : 0            TCA(enable) :
NO
 65-127-OCTET              : 0                    Threshold : 0            TCA(enable) :
NO
 128-255-OCTET             : 0                    Threshold : 0            TCA(enable) :
NO
 256-511-OCTET             : 0                    Threshold : 0            TCA(enable) :
NO
 512-1023-OCTET            : 0                    Threshold : 0            TCA(enable) :
NO
 1024-1518-OCTET           : 0                    Threshold : 0            TCA(enable) :
NO
 IN-UCAST                  : 0                    Threshold : 0            TCA(enable) :
NO
 IN-MCAST                  : 0                    Threshold : 0            TCA(enable) :
NO
 IN-BCAST                  : 0                    Threshold : 0            TCA(enable) :
NO
 OUT-UCAST                 : 0                    Threshold : 0            TCA(enable) :
NO
```

```
 OUT-BCAST                 : 0                    Threshold : 0           TCA(enable) :
NO
 OUT-MCAST                 : 0                    Threshold : 0           TCA(enable) :
NO
 TX-PKT                    : 1337921648           Threshold : 0           TCA(enable) :
NO
 OUT-OCTET                 : 1412845260584        Threshold : 100000      TCA(enable) :
NO
 IFIN-ERRORS               : 0                    Threshold : 0           TCA(enable) :
NO
 IFIN-OCTETS               : 0                    Threshold : 0           TCA(enable) :
NO
 STAT-MULTICAST-PKT        : 0                    Threshold : 0           TCA(enable) :
NO
 STAT-BROADCAST-PKT        : 0                    Threshold : 0           TCA(enable) :
NO
 STAT-UNDERSIZED-PKT       : 0                    Threshold : 0           TCA(enable) :
NO
 IN_GOOD_BYTES             : 0                    Threshold : 0           TCA(enable) :
NO
 IN_GOOD_PKTS              : 0                    Threshold : 0           TCA(enable) :
NO
 IN_DROP_OTHER             : 0                    Threshold : 0           TCA(enable) :
NO
 IN_ERROR_FRAGMENTS        : 0                    Threshold : 0           TCA(enable) :
NO
 IN_PKT_64_OCTET           : 0                    Threshold : 0           TCA(enable) :
NO
 IN_PKTS_65_127_OCTETS     : 0                    Threshold : 0           TCA(enable) :
NO
 IN_PKTS_128_255_OCTETS    : 0                    Threshold : 0           TCA(enable) :
NO
 IN_PKTS_256_511_OCTETS    : 0                    Threshold : 0           TCA(enable) :
NO
 IN_PKTS_512_1023_OCTETS   : 0                    Threshold : 0           TCA(enable) :
NO
 IN_PKTS_1024_1518_OCTETS  : 0                    Threshold : 0           TCA(enable) :
NO
 TX_UNDERSIZED_PKT         : 0                    Threshold : 0           TCA(enable) :
NO
 TX_OVERSIZED_PKT          : 0                    Threshold : 0           TCA(enable) :
NO
 TX_FRAGMENTS              : 0                    Threshold : 0           TCA(enable) :
NO
 TX_JABBER                 : 0                    Threshold : 0           TCA(enable) :
NO
 TX_BAD_FCS                : 0                    Threshold : 0           TCA(enable) :
NO
```

Example

```
ios#show controllers macSecCtrlr 0/0/0/16/2 pm current 30-sec macsec-secy-if
```

Displays the current performance monitoring parameters of the controller in macsec-secy-if mode in 30 sec intervals.

```
Macsec-Secy-If in the current interval [10:18:30 - 10:18:57 Sat Apr 22 2017]
Macsec-Secy-If current bucket type : Valid
InPktsUntagged     : 0                    Threshold : 0          TCA(enable) : NO
InPktsNoTag        : 0                    Threshold : 0          TCA(enable) : NO
InPktsBadTag       : 0                    Threshold : 0          TCA(enable) : NO
InPktsUnknownSCI   : 0                    Threshold : 0          TCA(enable) : NO
InPktsNoSCI        : 0                    Threshold : 0          TCA(enable) : NO
InPktsOverrun      : 0                    Threshold : 0          TCA(enable) : NO
InOctetsValidated  : 0                    Threshold : 0          TCA(enable) : NO
```

```
InOctetsDecrypted  : 321909392           Threshold : 0          TCA(enable) : NO
OutPktsUntagged    : 0                   Threshold : 0          TCA(enable) : NO
OutPktsTooLong     : 0                   Threshold : 0          TCA(enable) : NO
OutOctetsProtected : 0                   Threshold : 0          TCA(enable) : NO
OutOctetsEncrypted : 415501264           Threshold : 0          TCA(enable) : NO
```

Example

```
ios#show controllers macSecCtrlr 0/0/0/16/2 pm current 15-min macsec-secy-if
```

Displays the current performance monitoring parameters of the controller in macsec-secy-if mode in 15 minute intervals.

```
RP/0/RP0/CPU0:ios#show controllers macSecCtrlr 0/0/0/16/2 pm current 15-min macsec-secy-if
Sat Apr 22 10:18:40.743 UTC
Macsec-Secy-If in the current interval [10:15:00 - 10:18:40 Sat Apr 22 2017]
Macsec-Secy-If current bucket type : Valid
 InPktsUntagged     : 0                   Threshold : 0          TCA(enable) : NO
 InPktsNoTag        : 0                   Threshold : 0          TCA(enable) : NO
 InPktsBadTag       : 0                   Threshold : 0          TCA(enable) : NO
 InPktsUnknownSCI   : 0                   Threshold : 0          TCA(enable) : NO
 InPktsNoSCI        : 0                   Threshold : 0          TCA(enable) : NO
 InPktsOverrun      : 0                   Threshold : 0          TCA(enable) : NO
 InOctetsValidated  : 0                   Threshold : 0          TCA(enable) : NO
 InOctetsDecrypted  : 2541082096          Threshold : 0          TCA(enable) : NO
 OutPktsUntagged    : 0                   Threshold : 0          TCA(enable) : NO
 OutPktsTooLong     : 0                   Threshold : 0          TCA(enable) : NO
 OutOctetsProtected : 0                   Threshold : 0          TCA(enable) : NO
 OutOctetsEncrypted : 3279875344          Threshold : 0          TCA(enable) : NO
```

Example

```
ios#show controllers macSecCtrlr 0/0/0/16/2 pm current 30-sec  macsec-secy-tx
```

Displays the current performance monitoring parameters of the controller in macsec-secy-tx mode in 30 minute intervals.

```
Macsec-Secy-Tx in the current interval [10:18:30 - 10:18:59 Sat Apr 22 2017]
Macsec-Secy-Tx current bucket type : Valid
OutPktsProtected   : 0                   Threshold : 0          TCA(enable) : NO
OutPktsEncrypted   : 286527              Threshold : 0          TCA(enable) : NO
OutOctetsProtected : 0                   Threshold : 0          TCA(enable) : NO
OutOctetsEncrypted : 430363554           Threshold : 0          TCA(enable) : NO
OutPktsTooLong     : 0                   Threshold : 0          TCA(enable) : NO
```

Displays the current performance monitoring parameters of the controller in macsec-secy-tx mode in 24-hour interval.

```
RP/0/RP0/CPU0:ios#show controllers macSecCtrlr 0/0/0/24/3 pm current 24-hour macsec-secy-tx
Sat Apr  1 15:38:30.158 IST
Macsec-Secy-Tx in the current interval [00:00:00 - 15:38:30 Sat Apr 1 2017]
Macsec-Secy-Tx current bucket type : Valid
OutPktsProtected   : 0                   Threshold : 0          TCA(enable) : NO
OutPktsEncrypted   : 3160983513          Threshold : 0          TCA(enable) : NO
OutOctetsProtected : 0                   Threshold : 0          TCA(enable) : NO
OutOctetsEncrypted : 31559259393792      Threshold : 0          TCA(enable) : NO
OutPktsTooLong     : 0                   Threshold : 0          TCA(enable) : NO
```

Displays the current performance monitoring parameters of the controller in macsec-secy-rx mode in 24-hour interval.

```
RP/0/RP0/CPU0:ios#show controllers macSecCtrlr 0/0/0/10/3 pm current 24-hour macsec-secy-rx
Sat Apr  1 15:38:00.820 IST
Macsec-Secy-Rx in the current interval [00:00:00 - 15:38:01 Sat Apr 1 2017]
Macsec-Secy-Rx current bucket type : Valid
```

```
InPktsUnchecked   : 0                  Threshold : 0          TCA(enable) : NO
InPktsDelayed     : 0                  Threshold : 0          TCA(enable) : NO
InPktsLate        : 0                  Threshold : 0          TCA(enable) : NO
InPktsInvalid     : 0                  Threshold : 0          TCA(enable) : NO
InPktsOK          : 3159299558         Threshold : 0          TCA(enable) : NO
InPktsNotValid    : 0                  Threshold : 0          TCA(enable) : NO
InPktsNotUsingSA  : 0                  Threshold : 0          TCA(enable) : NO
InPktsUnusedSA    : 0                  Threshold : 0          TCA(enable) : NO
InPktsUntaggedHit : 0                  Threshold : 0          TCA(enable) : NO
InOctetsValidated : 0                  Threshold : 0          TCA(enable) : NO
InOctetsDecrypted : 31542446787072     Threshold : 0          TCA(enable) : NO
```

MACsec MKA Using EAP-TLS Authentication

Using IEEE 802.1X port-based authentication with Extensible Authentication Protocol (EAP-TLS), MACsec MKA can be configured between two NCS 1002 device ports. EAP-TLS allows mutual authentication and obtains MSK (master session key or primary session key). Both Connectivity Association Key Name (CKN) and connectivity association key (CAK) are derived from MSK for MKA operations. The device certificates are carried for authentication to the external AAA server using EAP-TLS.

IEEE 802.1X Device Roles

The devices in the network have the following specific roles with IEEE 802.1X authentication.

- Supplicant - An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.
- Authenticator - An entity that facilitates authentication of other entities attached to the same LAN.
- Authentication Server - An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the system in which the Authenticator resides.

Prerequisites for MACsec MKA Using EAP-TLS Authentication

- Ensure that a Certificate Authority (CA) server is configured for the network.
- Ensure a valid CA certificate.
- Ensure that the user has configured Cisco Identity Services Engine (ISE) Release 2.2 onwards or Cisco Secure Access Control Server Release 5.6 onwards as external AAA server.
- It is always good to have the NCS 1002 devices, the CA server, and the external AAA/Radius server synchronized using Network Time Protocol (NTP) Server. If clock is not synchronized, there might be instances where certificate validation will not be successful, due to timing issues.

  However, there is no dependency on the timezone between NCS 1002 devices, the CA Server and the external AAA/Radius server.

Configure MACsec Encryption Using EAP-TLS Authentication

Configuring MACsec encryption using EAP-TLS authentication involves the following tasks:

- Configure RADIUS Server, on page 69
- Configure 802.1X Authentication Method, on page 70
- Generate RSA Key Pair, on page 71
- Configure Trust Point, on page 71
- Authenticate Certificate Authority and Request Certificates, on page 72
- Configure EAP Profile, on page 73
- Configure 802.1X Profile, on page 74
- Configure EAP and 802.1X Profile on MACsec Controller, on page 75
- Verify EAP and 802.1X Configuration on MACsec Controller, on page 76

Configure RADIUS Server

configure

radius-server host {*IPv4 address of RADIUS server*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**key** *string*]

radius-server vsa attribute ignore unknown

exit

commit

Examples

The following is a sample of configuring the RADIUS server.

```
configure
radius-server host 209.165.200.225 auth-port 1645 acct-port 1646 key cisco
radius-server vsa attribute ignore unknown
exit
commit
```

The following is sample output of **show radius** command.

```
Tue Jun 27 10:39:20.851 IST
Global dead time: 0 minute(s)
Number of Servers: 1

Server: 209.165.200.225  is UP
  Address family: IPv4
  Total Deadtime: 0s Last Deadtime: 0s
  Timeout: 5 sec, Retransmit limit: 3
  Quarantined: No
  Authentication:
```

```
  42 requests, 0 pending, 0 retransmits
  6 accepts, 0 rejects, 0 challenges
  0 timeouts, 0 bad responses, 0 bad authenticators
  0 unknown types, 0 dropped, 361 ms latest rtt
  Throttled: 0 transactions, 0 timeout, 0 failures
  Estimated Throttled Access Transactions: 0
  Maximum Throttled Access Transactions: 0

  Automated TEST Stats:
      0 requests, 0 timeouts, 0 response, 0 pending
Accounting:
  0 requests, 0 pending, 0 retransmits
  0 responses, 0 timeouts, 0 bad responses
  0 bad authenticators, 0 unknown types, 0 dropped
  0 ms latest rtt
  Throttled: 0 transactions, 0 timeout, 0 failures
  Estimated Throttled Accounting Transactions: 0
  Maximum Throttled Accounting Transactions: 0

  Automated TEST Stats:
      0 requests, 0 timeouts, 0 response, 0 pending
```

Associated Commands

- radius-server
- radius-server host

Configure 802.1X Authentication Method

This procedure allows the user to configure 802.1X authentication method using RADIUS as the protocol. 802.1X authentication configuration allows to configure non-default profiles. However, only default is supported in NCS 1002.

configure

aaa authentication dot1x default group radius

exit

commit

Examples

The following is a sample of configuring the 802.1X authentication method.

```
configure
aaa authentication dot1x default group radius
exit
commit
```

The following is sample output of **show run aaa** command.

```
Tue Jun 27 10:39:17.437 IST
radius-server vsa attribute ignore unknown
radius-server host 209.165.200.225 auth-port 1645 acct-port 1646 key cisco
aaa authentication dot1x default group radius
```

Associated Commands

- aaa authentication dot1x

Generate RSA Key Pair

RSA key pairs are used to sign and encrypt key management messages. This is required before the you can obtain a certificate for the node.

configure

crypto key generate rsa [**usage-keys** | **general-keys**] [*keypair-label*]

exit

commit

Examples

The following is a sample of generating the RSA key pair.

```
configure
crypto key generate rsa ncs1k
exit
commit
```

The following is sample output of **show crypto key** *key-name* **rsa** command.

```
Tue Jun 27 10:39:44.152 IST
Key label: ncs1k
Type     : RSA General purpose
Size     : 2048
Created  : 10:02:32 IST Tue Jun 27 2017
Data     :
 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
 00B59CFD DF2A2AEF B5B3DB63 AED2F5CB 9C02E519 E379099C F24543E0 4F19310F
 1F7B981E 3520C20E D7934082 D9BF04D7 07E5824F EA5EA1BB DDDFF6CD 9FCBDF75
 F3EF39DA C08B7C69 40AC89D4 58FF3FD0 1ED2AC8C 770C2339 E8508B48 E648A15D
 FE3DE9FA 05E878B2 3094E2F8 8F6280C3 469FF22F 386483FC 5EDE8178 5F7537C6
 7B5C487E 7E6BC636 2EBC55E4 3A6264CE A113BE64 A20F47F0 E1AA603E D5DB078F
 A0B0F36E 4314C435 2283D93F 40B4FEEE 63C33968 DB399B2C 88D97ADE F8DF6ED9
 2CAD24BD FA86CF36 247DE466 E2622D79 B25779D3 FADFDDE2 70474236 2FD58F5A
 67D6CC24 38DE7C8F 33923479 E822E92D C9B141FF E576C59C 50BB3CC5 F693A7D4
 81020301 0001
```

Associated Commands

- crypto key generate rsa

Configure Trust Point

configure

crypto ca trustpoint {*ca-name*}

enrollment url {*ca-url*}

subject-name {*x.500-name*}

rsakeypair{*keypair-label*}

crl optional

exit

commit

Examples

The following is a sample of configuring the trust point.

```
configure
crypto ca trustpoint ncs1k
enrollment url http://209.165.200.226
subject-name CN=ncs1k,OU=BU,O=Govt,L=Newyork,ST=NY,C=US
rsakeypair ncs1k
crl optional
exit
commit
```

The following is sample output of **show run crypto ca trustpoint** *ca-name* command.

```
Tue Jun 27 10:39:40.375 IST
crypto ca trustpoint ncs1k
 crl optional
 subject-name CN=ncs1k,OU=BU,O=Govt,L=Newyork,ST=NY,C=US
 enrollment url http://209.165.200.226
 rsakeypair ncs1k
!
```

Associated Commands

- crypto ca truspoint
- enrollment url
- rsakeypair

Authenticate Certificate Authority and Request Certificates

This procedure authenticates the certificate authority (CA) with NCS 1002 and requests certificates from the CA. NCS 1002 must authenticate the CA by obtaining the self-signed certificate of the CA. The self-signed certificate contains the public key of the CA. It is required to manually authenticate the public key of the CA by contacting the CA administrator to compare the fingerprint of the CA certificate.

configure

crypto ca authenticate {*ca-name*}

crypto ca enroll {*ca-name*}

exit

commit

Examples

The following is a sample of authenticating the certificate authority and requesting certificates.

```
configure
crypto ca authenticate ncs1k
crypto ca enroll ncs1k
exit
commit
```

The following is sample output of **show crypto ca certificates** command.

```
Tue Jun 27 10:39:47.356 IST

Trustpoint       : ncs1k
==================================================
CA certificate
  Serial Number  : 01
  Subject:
        CN=ncs1k,OU=BU,O=Govt,L=Newyork,ST=NY,C=US
  Issued By      :
        CN=ncs1k,OU=BU,O=Govt,L=Newyork,ST=NY,C=US
  Validity Start : 03:50:38 UTC Wed Mar 22 2017
  Validity End   : 03:50:38 UTC Sat Mar 21 2020
  SHA1 Fingerprint:
         0B2E1F69BB42CE068AAB67F1C2C09C9FAF5F3F66
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : 01:1F
  Subject:
        serialNumber=cf302761,unstructuredAddress=209.165.200.226,unstructuredName=ncs1k,
        C=US,ST=NY,L=Newyork,O=Govt,OU=BU,CN=ncs1k
  Issued By      :
        CN=ncs1k,OU=BU,O=Govt,L=Newyork,ST=NY,C=US
  Validity Start : 04:37:11 UTC Tue Jun 27 2017
  Validity End   : 04:37:11 UTC Wed Jun 27 2018
  SHA1 Fingerprint:
         AF640E4E9E0521217BF3F4770465FD832B2AE90B
Associated Trustpoint: ncs1k
```

Associated Commands

- crypto ca authenticate
- crypto ca enroll

Configure EAP Profile

You can configure multiple EAP profiles.

configure

eap profile {*name*}

identity {*user-name*}

method tls pki-trustpoint {*trustpoint-name*}

exit

commit

Examples

The following is a sample of configuring the EAP profile.

```
configure
eap profile ncs1k
identity PRO67
method tls pki-trustpoint ncs1k
exit
commit
```

The following is sample output of **show run eap** command.

```
Tue Jun 27 10:39:51.211 IST
eap profile ncs1k
 method tls
  pki-trustpoint ncs1k
 !
 identity PRO67
!
```

Associated Commands

- eap profile
- pki-trustpoint

Configure 802.1X Profile

You can configure multiple 802.1X profiles. The role of the node running 802.1X profile can be supplicant, authenticator, or both.

configure

dot1x profile {*name*}

pae {**authenticator** | **supplicant** | **both**}

authentication timer reauthenticate {*seconds* | **server**}

supplicant eap profile {*profile-name*}

exit

commit

Examples

The following is a sample of configuring the 802.1X profile.

```
configure
dot1x profile reauth
pae both
authentication timer reauthenticate 3600
supplicant eap profile ncs1k
exit
commit
```

The following is sample output of **show run dot1x** command.

```
Tue Jun 27 10:39:55.178 IST
dot1x profile both_local_reauth
 pae both
 authenticator
  timer reauth-time 3600
 !
 supplicant
  eap profile ncs1k
 !
!
```

Associated Commands

- dot1x profile
- authentication timer reauthenticate
- dot1x supplicant eap profile

Configure EAP and 802.1X Profile on MACsec Controller

You can attach one of the 802.1X profiles on the MACsec controller.

configure

controller MACSecCtrl *Rack/Slot/Instance/Port*

dot1x profile *profile-name*

macsec eap [**policy** *macsec-policy-name*]

exit

commit

Example

The following is a sample of configuring MACsec EAP and 802.1X profile on the MACsec controller.

```
configure
controller MACSecCtrl 0/0/0/24
dot1x profile reauth
macsec eap
exit
commit
```

Associated Commands

- dot1x profile
- macsec eap

Verify EAP and 802.1X Configuration on MACsec Controller

show run controller mACSecCtrlr *Rack/Slot/Instance/Port*

```
Tue Jun 27 10:39:59.148 IST
controller MACSecCtrlr0/0/0/24
 dot1x profile both_local_reauth
 macsec eap
!
```

show dot1x controller mACSecCtrlr *Rack/Slot/Instance/Port* **detail**

```
Tue Jun 27 10:40:02.648 IST

Dot1x info for MACSecCtrlr0/0/0/24
----------------------------------------------------------------
Interface short name      : MS0/0/0/24
Interface handle          : 0x8000544
Interface MAC             : 2c00.4314.5c6c
Ethertype                 : 888E
PAE                       : Both
Dot1x Port Status         : AUTHORIZED
Dot1x Profile             : both_local_reauth
Supplicant:
   Config Dependency      : Resolved
   Eap profile            : ncs1k
   Client List:
      Authenticator       : 2c02.dc14.636c
      EAP Method          : EAP-TLS
      Supp SM State       : Authenticated
      Supp Bend SM State  : Idle
      Last authen time    : 2017 Jun 27 209.165.200.227
Authenticator:
   Config Dependency      : Resolved
   ReAuth                 : Enabled, 0 day(s), 01:00:00
   Client List:
      Supplicant          : 2c02.dc14.636c
      Auth SM State       : Authenticated
      Auth Bend SM State  : Idle
      Last authen time    : 2017 Jun 27 209.165.200.225
      Time to next reauth : 0 day(s), 00:46:09
MKA Interface:
   Dot1x Tie Break Role   : Auth
   EAP Based Macsec       : Enabled
   MKA Start time         : 2017 Jun 27 209.165.200.227
   MKA Stop time          : NA
   MKA Response time      : 2017 Jun 27 209.165.200.226
```

show macsec mka session controller mACSecCtrlr *Rack/Slot/Instance/Port*

```
Tue Jun 27 10:40:07.492 IST
```

```
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI            : 2c00.4314.5c6c/0018
Local Tx-SSCI           : 2
Interface MAC Address   : 2c00.4314.5c6c
MKA Port Identifier     : 24
Interface Name          : MS0/0/0/24
CAK Name (CKN)          : A3B6509EC0EBCAE8D610139669952E0A
CA Authentication Mode  : EAP
Keychain                : NA (EAP mode)
Member Identifier (MI)  : C12DD7CF165438D8B1732211
Message Number (MN)     : 422
Authenticator           : YES
Key Server              : YES
MKA Cipher Suite        : AES-128-CMAC

Latest SAK Status       : Rx & Tx
Latest SAK AN           : 0
Latest SAK KI (KN)      : C12DD7CF165438D8B1732211100000001 (1)
Old SAK Status          : FIRST-SAK
Old SAK AN              : 0
Old SAK KI (KN)         : FIRST-SAK (0)

SAK Transmit Wait Time  : 0s (Not waiting for any peers to respond)
SAK Retire Time         : 0s (No Old SAK to retire)
Time to SAK Rekey       : NA

MKA Policy Name         : *DEFAULT POLICY*
Key Server Priority     : 16
Delay Protection        : FALSE
Replay Window Size      : 64
Include ICV Indicator   : FALSE
Confidentiality Offset  : 0
Algorithm Agility       : 80C201
SAK Cipher Suite        : 0080C20001000004 (GCM-AES-XPN-256)
MACsec Capability       : 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired          : YES

# of MACsec Capable Live Peers           : 1
# of MACsec Capable Live Peers Responded : 1

Live Peer List:
  MI                        MN          Rx-SCI (Peer)        SSCI KS-Priority
  ------------------------------------------------------------------------------
  578656B568B072819160DCD4         420  2c02.dc14.636c/0018     1          16

Potential Peer List:
  MI                        MN          Rx-SCI (Peer)        SSCI KS-Priority
  ------------------------------------------------------------------------------
```

show macsec mka session

```
Tue Jun 27 10:40:59.320 IST
NODE: node0_RP0_CPU0
================================================================================
      Interface         Local-TxSCI       # Peers   Status  Key-Server
================================================================================
     MS0/0/0/24      2c00.4314.5c6c/0018      1     Secured    YES
```

CHAPTER 6

Configuring GMPLS UNI

The primary function of Generalized Multiprotocol Label Switching (GMPLS) User Network Interface (UNI) is to create circuit connection between two clients (UNI-C) of an optical network. This is achieved by signaling exchanges between UNI Client (UNI-C) and UNI Network (UNI-N) nodes. NCS 1002 node acts as UNI-C and NCS 2000 series node acts as UNI-N in GMPLS-UNI reference model.

The user can create a GMPLS optical channel trail (OCH Trail) in a network where the NCS 1002 node is connected to a NCS 2000 series node. The OCH trail circuit originates from a NCS 1002 trunk interface (UNI-C) on the source NCS 1002 node and terminates on the NCS 2000 series interface (UNI-N) on the destination NCS 2000 series node to create an optical connection. The prerequisite for the OCH trail circuit is to create a Link Management Protocol (LMP) link between the optical channel Add/Drop NCS 2000 series interface on the NCS 2000 series node and the NCS 1002 interface on the NCS 1002 node.

GMPLS UNI is supported only on the 100G and 200G trunk ports of the NCS 1002 node until R6.2.1. GMPLS UNI is supported on the 250G trunk port of the NCS 1002 node from R6.3.2.

Channel Spacing

DWDM grid (C-band: 1530 nm to 1569 nm) in optical spectrum can be divided into multiple channels so that each channel can carry data traffic independently. These channels can be separated with available slot widths called channel spacing.

GMPLS has two types of channel spacing.

- Fixed Grid channel spacing - The channel spacing is fixed to either 100 GHz, 50 GHz, or 12.5 GHz. NCS 1002 supports 50 GHz channel spacing.
- Flexible Grid channel spacing - The channels are divided in finer slices. The flexibility in channel spacing allows to transmit mixed bit-rate or mixed modulation data in a grid with different channel widths. It also helps in effective usage of DWDM grid with minimal wastage of spectral bandwidth. NCS 1002 supports 6.25 GHz channel spacing.

GMPLS UNI is supported only for fixed grid until R6.2.1. Hence, 250G channels from NCS 1002 node cannot pass through the NCS 2000 series node because of spectral issues of 50 GHz spacing. GMPLS UNI flexible grid is suported from R6.3.2 that suports 250G channels.

Prerequisites

- NCS 1002 node must have both the MPLS and MPLS-TE packages.
- NCS 2000 series node must have a valid license for ROADM and WSON support.

- The management IPs of NCS 1002 and NCS 2000 series nodes on both the source and destination must be reachable.

Limitations of GMPLS Flexible Grid

Flexible grid interoperability between R6.3.2 of NCS 1002 and R10.8 of NCS 2000 works for LMP discovery, flexible grid based wavelength assignment, and E2E tunnels.

However, there are interoperability issues with NCS 2000 at the following UNI revert and restoration scenarios.

- UNI-revert does not work for tunnels with XRO configurations.
- Restoration does not work due to wrong carrier allocation.

Configure GMPLS UNI

Configuring GMPLS UNI involves the following tasks:

The following configurations must be performed on the NCS 2000 series node.

1. Configure LMP and Alien Wavelength in NCS 2000 Series Node, on page 82
2. Retrieve Ifindex from NCS 2000 Series Node, on page 83

The following configurations must be performed on the NCS 1002 node.

1. Configure LMP in Cisco NCS 1002, on page 84
2. Configure RSVP in NCS 1002, on page 84
3. Configure MPLS Tunnel in NCS 1002, on page 85

GMPLS UNI Command Reference

For detailed command information about GMPLS UNI commands, see Cisco IOS XR MPLS Command Reference.

Debuggability

For any software issues, it is recommended to collect the output of show tech of (mpls, mpls-te, rsvp, cf-mgr, sysdb, ncs1k) for head node and tail node.

- Configuring GMPLS UNI, on page 81
- Configure LMP and Alien Wavelength in NCS 2000 Series Node, on page 82
- Configure Unnumbered LMP in NCS 2000 Series Node, on page 83
- Retrieve Ifindex from NCS 2000 Series Node, on page 83
- Configure LMP in Cisco NCS 1002, on page 84
- Configure RSVP in NCS 1002, on page 84
- Configure MPLS Tunnel in NCS 1002, on page 85
- Headless Mode and GMPLS UNI, on page 85
- Display GMPLS UNI Tunnel, RSVP, and LMP Information, on page 85
- Example of MPLS Tunnel Creation Without ERO, on page 90
- Example of MPLS Tunnel Creation with ERO, on page 91
- Example of MPLS Tunnel Creation with XRO, on page 92

• Example of MPLS Tunnel Creation with Explicit Signaled Wavelength, on page 93
• Validate GMPLS Assigned Channel Number (6.25 Ghz) over Coherent DSP, on page 93

Configuring GMPLS UNI

The primary function of Generalized Multiprotocol Label Switching (GMPLS) User Network Interface (UNI) is to create circuit connection between two clients (UNI-C) of an optical network. This is achieved by signaling exchanges between UNI Client (UNI-C) and UNI Network (UNI-N) nodes. NCS 1002 node acts as UNI-C and NCS 2000 series node acts as UNI-N in GMPLS-UNI reference model.

The user can create a GMPLS optical channel trail (OCH Trail) in a network where the NCS 1002 node is connected to a NCS 2000 series node. The OCH trail circuit originates from a NCS 1002 trunk interface (UNI-C) on the source NCS 1002 node and terminates on the NCS 2000 series interface (UNI-N) on the destination NCS 2000 series node to create an optical connection. The prerequisite for the OCH trail circuit is to create a Link Management Protocol (LMP) link between the optical channel Add/Drop NCS 2000 series interface on the NCS 2000 series node and the NCS 1002 interface on the NCS 1002 node.

GMPLS UNI is supported only on the 100G and 200G trunk ports of the NCS 1002 node until R6.2.1. GMPLS UNI is supported on the 250G trunk port of the NCS 1002 node from R6.3.2.

Channel Spacing

DWDM grid (C-band: 1530 nm to 1569 nm) in optical spectrum can be divided into multiple channels so that each channel can carry data traffic independently. These channels can be separated with available slot widths called channel spacing.

GMPLS has two types of channel spacing.

- Fixed Grid channel spacing - The channel spacing is fixed to either 100 GHz, 50 GHz, or 12.5 GHz. NCS 1002 supports 50 GHz channel spacing.
- Flexible Grid channel spacing - The channels are divided in finer slices. The flexibility in channel spacing allows to transmit mixed bit-rate or mixed modulation data in a grid with different channel widths. It also helps in effective usage of DWDM grid with minimal wastage of spectral bandwidth. NCS 1002 supports 6.25 GHz channel spacing.

GMPLS UNI is supported only for fixed grid until R6.2.1. Hence, 250G channels from NCS 1002 node cannot pass through the NCS 2000 series node because of spectral issues of 50 GHz spacing. GMPLS UNI flexible grid is suported from R6.3.2 that suports 250G channels.

Prerequisites

- NCS 1002 node must have both the MPLS and MPLS-TE packages.
- NCS 2000 series node must have a valid license for ROADM and WSON support.
- The management IPs of NCS 1002 and NCS 2000 series nodes on both the source and destination must be reachable.

Limitations of GMPLS Flexible Grid

Flexible grid interoperability between R6.3.2 of NCS 1002 and R10.8 of NCS 2000 works for LMP discovery, flexible grid based wavelength assignment, and E2E tunnels.

However, there are interoperability issues with NCS 2000 at the following UNI revert and restoration scenarios.

- UNI-revert does not work for tunnels with XRO configurations.
- Restoration does not work due to wrong carrier allocation.

Configure GMPLS UNI

Configuring GMPLS UNI involves the following tasks:

The following configurations must be performed on the NCS 2000 series node.

1. Configure LMP and Alien Wavelength in NCS 2000 Series Node, on page 82
2. Retrieve Ifindex from NCS 2000 Series Node, on page 83

The following configurations must be performed on the NCS 1002 node.

1. Configure LMP in Cisco NCS 1002, on page 84
2. Configure RSVP in NCS 1002, on page 84
3. Configure MPLS Tunnel in NCS 1002, on page 85

GMPLS UNI Command Reference

For detailed command information about GMPLS UNI commands, see Cisco IOS XR MPLS Command Reference.

Debuggability

For any software issues, it is recommended to collect the output of show tech of (mpls, mpls-te, rsvp, cf-mgr, sysdb, ncs1k) for head node and tail node.

Configure LMP and Alien Wavelength in NCS 2000 Series Node

This procedure creates a static LMP link between a NCS 2000 series node and NCS 1002 node. Unnumbered LMP can be configured only through TL1. Numbered LMP can be configured through both CTC and TL1.

In unnumbered LMP, the tunnel is terminated in any of the links reaching the peer NCS 1002 node. The numbered LMP is recommended because NCS 1002 trunk connections must be symmetric.

The alien wavelength must be configured for the NCS 2000 series interface (UNI-N) before creating the MPLS tunnel from NCS 1002 node (UNI-C). As CTC does not manage the NCS 1002 node, the alien wavelength must be separately configured in the Add Drop ports of NCS 2000 series node.

See DLP-G800 Create an LMP Link Using CTC to configure LMP and alien wavelength in NCS 2000 series node.

Configure Unnumbered LMP in NCS 2000 Series Node

In unnumbered LMP, the tunnel is terminated in any of the links reaching the peer NCS 1002 node. The numbered LMP is recommended because NCS 1002 trunk connections must be symmetric.

Use the following command to configure the unnumbered LMP from the TL1 interface.

```
ENT-UNICFG:[<TID>]:<src>:<CTAG>::<rvrsaid>,<rsysip>,<rifcip>,<mstpip>,
<commip>,[<remoteifinfo>]:[VALMODE=<optval>],[VALZONE=<oprzone>],[ADMINSTATE=<adminstate>],
[RESTTYPE=<resttype>],[CKTLABEL=<cktlabel>],[USPWROFS=<upstrmpwr>],
[DSPWROFS=<dnstrmpwr>],[ALLOWREGEN=<allowregen>],
[UNICTRLMODE=<unictrlmode>],[REVERTMODE=<revertmode>],
[SOAK=<HH-MM-SS>],[RESTVALMODE=<restvalmode>,[RESTVALZONE=<restvalzone>],
[TERMINTFDX=<termintfdx>],[DIVERSITY=<diversity>],[DIVERSITYTYPE=<diversitytype>],
[ISLOOSE=<isloose>],[UNIMODE=<unimode>],[DESCR=<descr>],[ALIENID=<alienid>],
[FECMODE=<fecmode>],[TRUNKMODE=<trunkmode>],[OPTENDPOINT=<optendpoint>],
[PAIREDOPTENDPOINT=<pairedoptendpoint>],[REMOTEIFINFOLIST=<remoteifinfolist>],
[LMPTYPE=<lmptype>][:];
```

rvrsaid is the destination AID. *rsysip* is the remote system IP address. *rifcip* is the remote interface IP address and enter 0.0.0.0 for unnumbered LMP. *mstpip* is the MSTP interface IP address and enter 0.0.0.0 for unnumbered LMP. *commip* is the destination IP address.

Example

```
ENT-UNICFG::PLINE-20-5-RX:111::PLINE-20-5-TX,10.58.229.22,10.22.22.5,10.90.90.5,10.58.229.22,
"Unnumb":VALMODE=FULL,VALZONE=RED,DESCR=90_Porta5_int27_Rosco22_250_20%,ADMINSTATE=UP,RESTTYPE=NONE,
UNICTRLMODE=CLIENT,RESTVALMODE=NONE,UNIMODE=GMPLS,ALIENID=NCS1K,
FECMODE=SD-20,TRUNKMODE=250G,LMPTYPE=SIGNALED;
```

Retrieve Ifindex from NCS 2000 Series Node

The Ifindex of all the LMP ports of NCS 2000 series node can be retrieved using CTC or TL1.

Using CTC

The Ifindex of all the LMP ports of NCS 2000 series node in decimal format can be retrieved using CTC from the **Originating Interface Index** column under the **Provisioning** > **LMP** tabs.

Using TL1

1. Log in to the TL1 interface and issue the following command.
2. **rtrv-unicfg ::all:1;**

This command retrieves the Ifindex of all the LMP ports of NCS 2000 series node in hexadecimal. This must be converted to decimal and used in remote Ifindex of NCS 1002 node during the LMP configuration.

TL1 Output

```
PSLINE-81-1-9-RX:PSLINE-81-1-9-TX,10.77.142.92,10.3.3.4,10.3.3.3,0.0.0.0,VALMODE=NONE,ADMINSTATE=UP,
RESTTYPE=REVERT,USPWROFS=0.0,
DSPWROFS=0.0,ALLOWREGEN=NO,UNICTRLMODE=CLIENT,REVERTMODE=MANUAL,SOAK=00-01-00,
RESTVALMODE=NONE,TERMINTFDX=0,ORIGINTFIDX=7f000d12,NUMBERED=TRUE,UNIMODE=GMPLS
```

```
PSLINE-81-1-10-RX:PSLINE-81-1-10-TX,10.77.142.92,10.4.4.4,10.4.4.3,0.0.0.0,VALMODE=NONE,ADMINSTATE=UP,
RESTTYPE=REVERT,USPWROFS=0.0,DSPWROFS=0.0,ALLOWREGEN=NO,UNICTRLMODE=CLIENT,
REVERTMODE=MANUAL,SOAK=00-01-00,RESTVALMODE=NONE,TERMINTFDX=0,
ORIGINTFIDX=7f000d14,NUMBERED=TRUE,UNIMODE=GMPLS
```

The Ifindex of Port 81-1-9 is 7f000d12 (in hexadecimal) and 2130709778 (in decimal). The Ifindex of Port 81-1-10 is 7f000d14 (in hexadecimal) and 2130709780 (in decimal).

Configure LMP in Cisco NCS 1002

Link Management Protocol (LMP) is a logical link that must be created on the trunk optics controller on the source and destination NCS 1002 nodes of the tunnel. Only static LMP is supported.

As CTC does not manage the NCS 1002 node, the Ifindex of Add Drop ports of NCS 2000 series node must be manually retrieved through TL1 or CTC LMP panel and used in LMP configuration in NCS 1002. See Retrieve Ifindex from NCS 2000 Series Node, on page 83 to retrieve the Ifindex. This Ifindex must be converted to decimal and used in the **neighbor interface-id unnumbered** command node during the LMP configuration.

Numbered trail creation requires the management IP address, link IP address (IP address of the optics controller), and the interface index. Unnumbered trail creation requires the management IP address and the interface index.

link-id ipv4 unicast IP address is the IP address of the optics controller. **neighbor link-id ipv4 unicast** IP address is the IP address of the MSTP interface. **neighbor flexi-grid-capable** enables GMPLS UNI flexible grid channel spacing.

The following is a sample of configuring the LMP on the source NCS 1002 node.

show running-config lmp

```
lmp
gmpls optical-uni
  controller Optics0/0/0/13
   neighbor NCS1K
   neighbor link-id ipv4 unicast 192.0.2.3
   neighbor flexi-grid-capable
   neighbor interface-id unnumbered 19
   link-id ipv4 unicast 192.0.2.4
  !
  neighbor NCS1K
   ipcc routed
   router-id ipv4 unicast 192.0.2.1
  !
  router-id ipv4 unicast 192.0.2.2
!
!
```

Configure RSVP in NCS 1002

Resource Reservation Protocol (RSVP) configuration with appropriate timeout for optical network must be performed on the source and destination NCS 1002 nodes of the tunnel. The following is a sample of configuring RSVP on the source NCS 1002 node.

```
controller optics 0/0/0/6
```

```
signalling refresh out-of-band interval 3600
signalling refresh out-of-band missed 24
```

Configure MPLS Tunnel in NCS 1002

MPLS tunnels can be configured only from the 100G and 200G trunk ports of the NCS 1002 node. The trunk optics controller must be in **no shut** state.

The following is a sample of configuring the MPLS tunnel on the source NCS 1002 node.

```
mpls traffic-eng
    gmpls optical-uni
        controller optics 0/0/0/6
           tunnel-properties
              tunnel-id 100
              destination ipv4 unicast 10.20.20.20
              path-option 10 no-ero lockdown
```

Explicit Route Object (ERO) - Includes the route(s) to be used through a list of specified nodes for a tunnel.

Exclude Route Object (XRO) - Excludes the route(s) to be used through a list of specified nodes for a tunnel.

The following is a sample to enable the controller to participate in the MPLS tunnel on the destination NCS 1002 node.

```
mpls traffic-eng
    gmpls optical-uni
        controller optics 0/0/0/6
```

Headless Mode and GMPLS UNI

NCS 1002 can carry traffic with a non-functional CPU (headless mode) for up to 72 hours. The existing GMPLS UNI tunnels are not affected by headless events such as system reload and CPU OIR operation on NCS 1002 node. However, the existing GMPLS UNI tunnels are affected if changes to the tunnel are triggered by the peer device when NCS 1002 node operates in headless mode.

Display GMPLS UNI Tunnel, RSVP, and LMP Information

show mpls traffic-eng link-management optical-uni controller optics *0/0/0/13*

```
Mon Sep 25 10:58:02.018 UTC
Optical interface: Optics0/0/0/13
  Overview:
    IM state: Up
    Child interface: : IM state Unknown
    OLM/LMP state: Up
    Optical tunnel state: up
  Connection:
    Tunnel role: Head
    Tunnel-id: 32, LSP-id 144, Extended tunnel-id 10.77.142.93
    Tunnel source: 10.77.142.93, destination: 10.6.1.1
    Optical router-ids: Local: 10.77.142.93, Remote: 10.77.142.94
    Label source: UNI-N
```

```
  Upstream label:
    Optical label:
    Grid                : DWDM
    Channel spacing     : 6.25 GHz
    Identifier          : 0
    Channel Number      : 88
  Downstream label:
    Optical label:
    Grid                : DWDM
    Channel spacing     : 6.25 GHz
    Identifier          : 0
    Channel Number      : 88
  SRLG discovery: Disabled
  SRLG announcement: None
Admission Control:
  Upstream: Admitted (LSP ID: 144)
  Downstream: Admitted (LSP ID: 144)
OLM/LMP adjacency information:
  Adjacency status: Up
  Local:
    node ID: 10.77.142.93
    link interface ID: 19
    link ID: 10.5.1.1
  Neighbor:
    node ID: 10.77.142.94 (38-SIT3)
    link interface ID: 2130709792
    link ID: 10.5.1.2
    IPCC: Routed to 10.77.142.94
Optical capabilities:
  Controller type: DWDM
  Channel spacing: 6.25 GHz
  Default channel: 88
  776 supported channels:
    -295, -294, -293, -292, -291, -290, -289, -288
    -287, -286, -285, -284, -283, -282, -281, -280
    -279, -278, -277, -276, -275, -274, -273, -272
    -271, -270, -269, -268, -267, -266, -265, -264
    -263, -262, -261, -260, -259, -258, -257, -256
    -255, -254, -253, -252, -251, -250, -249, -248
    -247, -246, -245, -244, -243, -242, -241, -240
    -239, -238, -237, -236, -235, -234, -233, -232
    -231, -230, -229, -228, -227, -226, -225, -224
    -223, -222, -221, -220, -219, -218, -217, -216
    -215, -214, -213, -212, -211, -210, -209, -208
    -207, -206, -205, -204, -203, -202, -201, -200
    -199, -198, -197, -196, -195, -194, -193, -192
    -191, -190, -189, -188, -187, -186, -185, -184
    -183, -182, -181, -180, -179, -178, -177, -176
    -175, -174, -173, -172, -171, -170, -169, -168
    -167, -166, -165, -164, -163, -162, -161, -160
    -159, -158, -157, -156, -155, -154, -153, -152
    -151, -150, -149, -148, -147, -146, -145, -144
    -143, -142, -141, -140, -139, -138, -137, -136
    -135, -134, -133, -132, -131, -130, -129, -128
    -127, -126, -125, -124, -123, -122, -121, -120
    -119, -118, -117, -116, -115, -114, -113, -112
    -111, -110, -109, -108, -107, -106, -105, -104
    -103, -102, -101, -100, -99, -98, -97, -96
    -95, -94, -93, -92, -91, -90, -89, -88
    -87, -86, -85, -84, -83, -82, -81, -80
    -79, -78, -77, -76, -75, -74, -73, -72
    -71, -70, -69, -68, -67, -66, -65, -64
    -63, -62, -61, -60, -59, -58, -57, -56
    -55, -54, -53, -52, -51, -50, -49, -48
```

```
 -47, -46, -45, -44, -43, -42, -41, -40
 -39, -38, -37, -36, -35, -34, -33, -32
 -31, -30, -29, -28, -27, -26, -25, -24
 -23, -22, -21, -20, -19, -18, -17, -16
 -15, -14, -13, -12, -11, -10, -9, -8
 -7, -6, -5, -4, -3, -2, -1, 0
 1, 2, 3, 4, 5, 6, 7, 8
 9, 10, 11, 12, 13, 14, 15, 16
 17, 18, 19, 20, 21, 22, 23, 24
 25, 26, 27, 28, 29, 30, 31, 32
 33, 34, 35, 36, 37, 38, 39, 40
 41, 42, 43, 44, 45, 46, 47, 48
 49, 50, 51, 52, 53, 54, 55, 56
 57, 58, 59, 60, 61, 62, 63, 64
 65, 66, 67, 68, 69, 70, 71, 72
 73, 74, 75, 76, 77, 78, 79, 80
 81, 82, 83, 84, 85, 86, 87, 88
 89, 90, 91, 92, 93, 94, 95, 96
 97, 98, 99, 100, 101, 102, 103, 104
 105, 106, 107, 108, 109, 110, 111, 112
 113, 114, 115, 116, 117, 118, 119, 120
 121, 122, 123, 124, 125, 126, 127, 128
 129, 130, 131, 132, 133, 134, 135, 136
 137, 138, 139, 140, 141, 142, 143, 144
 145, 146, 147, 148, 149, 150, 151, 152
 153, 154, 155, 156, 157, 158, 159, 160
 161, 162, 163, 164, 165, 166, 167, 168
 169, 170, 171, 172, 173, 174, 175, 176
 177, 178, 179, 180, 181, 182, 183, 184
 185, 186, 187, 188, 189, 190, 191, 192
 193, 194, 195, 196, 197, 198, 199, 200
201, 202, 203, 204, 205, 206, 207, 208
 209, 210, 211, 212, 213, 214, 215, 216
 217, 218, 219, 220, 221, 222, 223, 224
 225, 226, 227, 228, 229, 230, 231, 232
 233, 234, 235, 236, 237, 238, 239, 240
 241, 242, 243, 244, 245, 246, 247, 248
 249, 250, 251, 252, 253, 254, 255, 256
 257, 258, 259, 260, 261, 262, 263, 264
 265, 266, 267, 268, 269, 270, 271, 272
 273, 274, 275, 276, 277, 278, 279, 280
 281, 282, 283, 284, 285, 286, 287, 288
 289, 290, 291, 292, 293, 294, 295, 296
 297, 298, 299, 300, 301, 302, 303, 304
 305, 306, 307, 308, 309, 310, 311, 312
 313, 314, 315, 316, 317, 318, 319, 320
 321, 322, 323, 324, 325, 326, 327, 328
 329, 330, 331, 332, 333, 334, 335, 336
 337, 338, 339, 340, 341, 342, 343, 344
 345, 346, 347, 348, 349, 350, 351, 352
 353, 354, 355, 356, 357, 358, 359, 360
 361, 362, 363, 364, 365, 366, 367, 368
 369, 370, 371, 372, 373, 374, 375, 376
 377, 378, 379, 380, 381, 382, 383, 384
 385, 386, 387, 388, 389, 390, 391, 392
 393, 394, 395, 396, 397, 398, 399, 400
 401, 402, 403, 404, 405, 406, 407, 408
 409, 410, 411, 412, 413, 414, 415, 416
 417, 418, 419, 420, 421, 422, 423, 424
 425, 426, 427, 428, 429, 430, 431, 432
 433, 434, 435, 436, 437, 438, 439, 440
 441, 442, 443, 444, 445, 446, 447, 448
 449, 450, 451, 452, 453, 454, 455, 456
 457, 458, 459, 460, 461, 462, 463, 464
```

```
      465, 466, 467, 468, 469, 470, 471, 472
      473, 474, 475, 476, 477, 478, 479, 480
    Controller SRLGs
      None
```

show mpls traffic-eng link-management optical-uni

Displays the summary of the GMPLS UNI tunnel state. MPLS tunnels are not created when the optics controller is in shutdown state. IM state is shown as "Admin down". Issue the **no shutdown** command under the controller interface to initiate the tunnel creation.

```
Mon Jan 11 04:57:46.220 UTC

System Information:
Optical Links Count: 1 (Maximum Links Supported 100)

Optical interface: Optics0/0/0/13
Overview:
IM state: Up
Child interface: : IM state Unknown
OLM/LMP state: Up
Optical tunnel state: up
Connection:
Tunnel role: Tail
Tunnel-id: 1, LSP-id 2, Extended tunnel-id 10.77.132.158
Tunnel source: 10.77.132.158, destination: 10.1.1.1
Optical router-ids: Local: 10.77.132.156, Remote: 10.77.132.158
Label source: UNI-N
Upstream label:
Optical label:
Grid : DWDM
Channel spacing : 50 GHz
Identifier : 0
Channel Number : -8
Downstream label:
Optical label:
Grid : DWDM
Channel spacing : 50 GHz
Identifier : 0
Channel Number : -8
SRLG discovery: Disabled
SRLG announcement: None
Admission Control:
Upstream: Admitted (LSP ID: 2)
Downstream: Admitted (LSP ID: 2)
OLM/LMP adjacency information:
Adjacency status: Up
Local:
node ID: 10.77.132.156
link interface ID: 6
link ID: 10.1.1.1
Neighbor:
node ID: 10.77.132.158 (RDT_2)
link interface ID: 19
link ID: 10.1.1.2
IPCC: Routed to 10.77.132.158
Optical capabilities:
Controller type: DWDM
Channel spacing: 50 GHz
Default channel: -7
97 supported channels:
-36, -35, -34, -33, -32, -31, -30, -29
-28, -27, -26, -25, -24, -23, -22, -21
```

```
-20, -19, -18, -17, -16, -15, -14, -13
-12, -11, -10, -9, -8, -7, -6, -5
-4, -3, -2, -1, 0, 1, 2, 3
4, 5, 6, 7, 8, 9, 10, 11
12, 13, 14, 15, 16, 17, 18, 19
20, 21, 22, 23, 24, 25, 26, 27
28, 29, 30, 31, 32, 33, 34, 35
36, 37, 38, 39, 40, 41, 42, 43
44, 45, 46, 47, 48, 49, 50, 51
52, 53, 54, 55, 56, 57, 58, 59
60
Controller SRLGs
None
```

show mpls traffic-eng link-management optical-uni tabular

Displays the summary of the GMPLS UNI tunnel state in tabular format.

```
Mon Jan 11 05:27:06.407 UTC

System Information:
Optical Links Count: 1 (Maximum Links Supported 100)

State LMP GMPLS tunnel
Interface       Admin    Oper       adjacency     role     tun-id  state
-------------------------------------------------------------------------
Op0/0/0/13       up       up           up         Tail       1      up
```

show mpls traffic-eng tunnels

Displays information about tunnels.

```
Mon Jan 11 05:30:44.501 UTC

LSP Tunnel 10.77.132.158 1 [8] is signalled, Signaling State: up
Tunnel Name: ios_ot1_10.1.1.1 Tunnel Role: Tail
Upstream label:
Optical label:
Grid : DWDM
Channel spacing : 50 GHz
Identifier : 0
Channel Number : -8
Downstream label:
Optical label:
Grid : DWDM
Channel spacing : 50 GHz
Identifier : 0
Channel Number : -8
Signalling Info:
Src 10.77.132.158 Dst 10.1.1.1, Tun ID 1, Tun Inst 8, Ext ID 10.77.132.158
Router-IDs: upstream 10.77.132.158
local 10.77.132.156
Priority: 7 7
SRLGs: not collected
Path Info:
Incoming Address: 10.1.1.2
Incoming:
Explicit Route:
No ERO

Route Exclusions:
No XRO
Record Route: Disabled
Tspec: avg rate=4294967033 kbits, burst=1000 bytes, peak rate=4294967033 kbits
```

```
Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
Resv Info: None
Record Route: Disabled
Fspec: avg rate=4294967033 kbits, burst=1000 bytes, peak rate=4294967033 kbits
Displayed 0 (of 0) heads, 0 (of 0) midpoints, 1 (of 1) tails
Displayed 0 up, 0 down, 0 recovering, 0 recovered heads
```

show rsvp neighbors

Displays information about RSVP neighbors.

```
Mon Jan 11 05:33:21.483 UTC
Global Neighbor: 10.77.132.158
Interface       Neighbor Interface
------------------- ---------------
10.77.132.158   MgmtEth0/RP0/CPU0/0
```

show lmp gmpls optical-uni

Verifies LMP configuration and state.

```
GMPLS Optical-UNI LMP Router ID: 10.77.132.156

LMP Neighbor
Name: RDT_2, IP: 10.77.132.158, Owner: GMPLS Optical-UNI
IPCC ID: 1, State Up
Known via : Configuration
Type : Routed
Destination IP : 10.77.132.158
Source IP : 10.77.132.156

Interface I/F | Lcl Interface ID | Lcl Link ID | Interface LMP state
----------------------+-------------------+----------------+-----------------------
Optics0/0/0/13     6                10.1.1.1           Up
```

Example of MPLS Tunnel Creation Without ERO

On the source NCS 1002 node:

```
lmp
gmpls optical-uni
controller Optics0/0/0/5
neighbor HUB-1
neighbor link-id ipv4 unicast 10.4.4.2
neighbor interface-id unnumbered 2130709780
link-id ipv4 unicast 10.4.4.1
neighbor HUB-1
ipcc routed
router-id ipv4 unicast 10.77.142.94
router-id ipv4 unicast 10.77.142.93
mpls traffic-eng
gmpls optical-uni
controller Optics0/0/0/5
tunnel-properties
tunnel-id 10
destination ipv4 unicast 10.4.4.4
path-option 10 no-ero lockdown
rsvp
controller Optics0/0/0/5
```

```
signalling refresh out-of-band interval 3600
signalling refresh out-of-band missed 24
```

On the destination NCS 1002 node:

```
lmp
gmpls optical-uni
controller Optics0/0/0/5
neighbor HUB-2
neighbor link-id ipv4 unicast 10.4.4.3
neighbor interface-id unnumbered 2130709780
link-id ipv4 unicast 10.4.4.4
neighbor HUB-2
ipcc routed
router-id ipv4 unicast 10.77.142.46
router-id ipv4 unicast 10.77.142.92
mpls traffic-eng
gmpls optical-uni
controller Optics0/0/0/5
rsvp
controller Optics0/0/0/6
signalling refresh out-of-band interval 3600
signalling refresh out-of-band missed 24
```

The following is the output of the **show mpls traffic-eng tunnels 10** command on the source NCS 1002 node.

```
Name: GMPLS-UNI-Optics0/0/0/5  Destination: 10.4.4.4
  Signalled-Name: HEADNODE_ot10_10.4.4.4
GMPLS UNI tunnel controlling link Optics0/0/0/5, tunnel-id: 10
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10, (LOCKDOWN) type no-ero  (Basis for Setup)
    Last Signalled Error : Tue Feb 14 02:19:01 2017
      Info: [11] PathErr(24,6)-(routing, unacceptable label object) at 10.4.4.2
    G-PID: 0x0800 (derived from egress interface properties)
    Creation Time: Tue Jan 10 15:07:11 2017 (4w6d ago)
  Config Parameters:
    Priority:  7  7 Affinity: 0x0/0xffff
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    SRLG discovery: Disabled
  History:
    Tunnel has been up for: 00:00:33 (since Tue Feb 14 02:19:02 IST 2017)
    Current LSP:
      Uptime: 00:00:33 (since Tue Feb 14 02:19:02 IST 2017)
Displayed 1 (of 4) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Example of MPLS Tunnel Creation with ERO

On the source NCS 1002 node:

```
mpls traffic-eng
      gmpls optical-uni
          controller Optics0/0/0/5
              tunnel-properties
                  tunnel-id 10
```

```
                destination ipv4 unicast 10.4.4.4
                path-option 10 explicit name ero-1 lockdown verbatim

explicit-path name ero-1
     index 10 next-address strict ipv4 unicast 10.4.4.2
     index 20 next-address strict ipv4 unicast 10.77.142.66
```

The following is the output of the **show mpls traffic-eng tunnels 10** command on the source NCS 1002 node.

```
Name: GMPLS-UNI-Optics0/0/0/5  Destination: 10.4.4.4
  Signalled-Name: HEADNODE_ot10_10.4.4.4
GMPLS UNI tunnel controlling link Optics0/0/0/5, tunnel-id: 10
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10, (LOCKDOWN verbatim) type explicit ero-1 (Basis for Setup)
    Last Signalled Error : Tue Feb 14 01:57:02 2017
      Info: [7] PathErr(24,6)-(routing, unacceptable label object) at 10.4.4.2
    G-PID: 0x0800 (derived from egress interface properties)
    Creation Time: Tue Jan 10 15:07:11 2017 (4w6d ago)
  Config Parameters:
    Priority:  7  7 Affinity: 0x0/0xffff
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    SRLG discovery: Disabled
  History:
    Tunnel has been up for: 00:09:19 (since Tue Feb 14 01:57:02 IST 2017)
    Current LSP:
      Uptime: 00:09:19 (since Tue Feb 14 01:57:02 IST 2017)

  Path info (No IGP):
  Hop0: 10.4.4.2
  Hop1: 10.77.142.66
Displayed 1 (of 4) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Example of MPLS Tunnel Creation with XRO

On the source NCS 1002 node:

```
mpls traffic-eng
      attribute-set xro xro-1
           exclude strict lsp source 10.77.132.93 destination 10.3.3.4 tunnel-id 22
extended-tunnel-id 10.77.132.93
           exclude strict srlg value 123123
      gmpls optical-uni
          controller Optics0/0/0/5
             tunnel-properties
                tunnel-id 10
                destination ipv4 unicast 10.4.4.4
                path-option 10 no-ero xro-attribute-set xro-1 lockdown
          controller Optics0/0/0/6
             tunnel-properties
                tunnel-id 22
                destination ipv4 unicast 10.3.3.4
                path-option 12 no-ero lockdown
```

The following is the output of the **show mpls traffic-eng tunnels 10** command on the source NCS 1002 node.

```
Name: GMPLS-UNI-Optics0/0/0/5  Destination: 10.4.4.4
  Signalled-Name: HEADNODE_ot10_10.4.4.4
GMPLS UNI tunnel controlling link Optics0/0/0/5, tunnel-id: 10
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10, (LOCKDOWN) type no-ero  (Basis for Setup)
      XRO attribute-set: xro-1
        Strict, SRLG id 123123
        Strict, P2P LSP, tun-id 22 lsp-id 0,Mutual-Div-flag 0 LSP-id ignored
          src 10.77.132.93, dest 10.3.3.4, ext-id 10.77.132.93
    Last Signalled Error : Tue Feb 14 02:09:13 2017
      Info: [8] PathErr(24,6)-(routing, unacceptable label object) at 10.4.4.2
    G-PID: 0x0800 (derived from egress interface properties)
    Creation Time: Tue Jan 10 15:07:11 2017 (4w6d ago)
  Config Parameters:
    Priority:  7  7 Affinity: 0x0/0xffff
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    SRLG discovery: Disabled
  History:
    Tunnel has been up for: 00:01:41 (since Tue Feb 14 02:09:13 IST 2017)
    Current LSP:
      Uptime: 00:01:41 (since Tue Feb 14 02:09:13 IST 2017)
Displayed 1 (of 4) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Example of MPLS Tunnel Creation with Explicit Signaled Wavelength

On the source NCS 1002 node:

```
gmpls optical-uni
     controller Optics0/0/0/5
         tunnel-properties
             tunnel-id 10
             destination ipv4 unicast 10.4.4.4
             path-option 10 no-ero signaled-label dwdm wavelength 22 lockdown
```

Validate GMPLS Assigned Channel Number (6.25 Ghz) over Coherent DSP

This procedure allows you to validate whether the channel number assigned through GMPLS is programmed in optics controller.

Step 1 **show mpls traffic-eng link-management optical-uni controller optics** *0/0/0/13*

This command provides the channel number assigned (say 88) and channel spacing (say 6.25 Ghz).

```
Mon Sep 25 10:58:02.018 UTC
```

```
Optical interface: Optics0/0/0/13
  Overview:
    IM state: Up
    Child interface: : IM state Unknown
    OLM/LMP state: Up
    Optical tunnel state: up
  Connection:
    Tunnel role: Head
    Tunnel-id: 32, LSP-id 144, Extended tunnel-id 10.77.142.93
    Tunnel source: 10.77.142.93, destination: 10.6.1.1
    Optical router-ids: Local: 10.77.142.93, Remote: 10.77.142.94
    Label source: UNI-N
    Upstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 6.25 GHz
      Identifier          : 0
      Channel Number      : 88
    Downstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 6.25 GHz
      Identifier          : 0
      Channel Number      : 88
    SRLG discovery: Disabled
    SRLG announcement: None
```

Step 2 **show controllers optics** *0/0/0/13* **dwdm-carrrier-map flexi-grid**

This command provides the mapping for the channel number (say 88) to respective frequency (say 193.65000) and wavelength (say 1548.115).

```
DWDM Carrier Band:: OPTICS_C_BAND
MSA ITU channel range supported: 1~97

DWDM Carrier Map table
-----------------------------------------------------
Channel     G.694.1     Frequency     Wavelength
index      Ch Num        (THz)          (nm)
-----------------------------------------------------
   393        88        193.65000      1548.115
```

Step 3 **show controllers optics** *0/0/0/13* **| inc Wavelength**

This command provides the wavelength present in optics controller for the specific trunk port.

```
Tue Nov  7 04:05:09.148 UTC
Wavelength= 1548.115
```

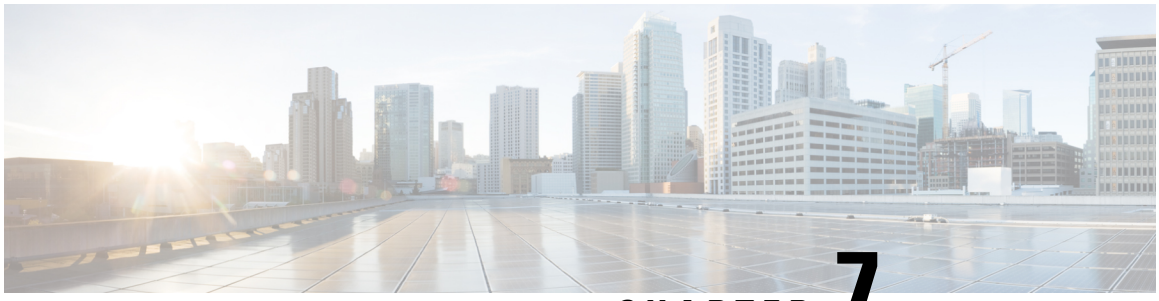
Step 4 **show hw-module slice 1 coherentDSP 13 config hardware | inc Frequency**

This command verifes the frequency obtained in step 3 with the frequency programmed in coherent DSP.

```
Tue Nov  7 04:07:35.449 UTC

**********COHERENT DSP 13**********
Device Configuration:
-Traffic mode: 16-QAM 250G 20%-FEC (0)
-Power Mode: High Power (1)
-Near End Loop: disabled (0)
-Far End Loop: disabled (0)
```

```
-Caui Bitrate: Ethernet (1)
-Caui Mode: 0x0006
-TX Laser Frequency:  193.65000
-TX Optical Output Power SetPoint: -1.50 dBm
-TX Caui Ports enabled: 0x00000007
-TX Output Power: enabled
-TX Differential Encoder: enabled
-Tx LsWavalm ConsAction: disabled
-RX Laser Frequency:  193.65000
-RX Caui Ports enabled: 0x00000007
-RX CD Start Value: -70000 ps/nm
-RX CD Stop Value: 70000 ps/nm
-RX PreFec Ber Raise Threhold: 1065353216.000000
-RX PreFec Ber Cease Threhold: 1065353216.000000
-RX Preemphasis: P: 0 R: 0 T: 0 Q: 0 S: 0 U: 0
-RX Differential Decoder: enabled
-RX SD-FEC Decoder: enabled
-RX Lock to Hold-On Clock: disabled
-RX Enable POWALM cons action: disabled
-TX MCLK: disabled
-Tx MCLK Rate: 1/32 of symbolrate (0)
-RX MCLK: disabled
-Rx MCLK Rate: 1/32 of symbolrate (0)
-RX PreFec Ber Raise Time Interval: 1.00 s
-RX PreFec Ber Cease Time Interval: 1.00 s
-TX Mapper: A: PortP_L1, B: PortP_L2, C: PortR_L1, D: PortR_L2, E: PortT_L1
-RX Demapper: A: PortP_L1, B: PortP_L2, C: PortR_L1, D: PortR_L2, E: PortT_L1
-TX Laser Fine Tuning: 0.0 GHz
-RX Laser Fine Tuning: 0.0 GHz
```



CHAPTER 7

Configuring Breakout Patch Panel

The client ports can operate at 10G mode using an external breakout patch panel.

- Breakout Patch Panel, on page 97
- Configure Breakout Patch Panel, on page 97

Breakout Patch Panel

The key features of the breakout patch panel are as follows:

- Has 20 MPO ports in the back side that can be connected to 20 QSFP+ client ports of NCS 1002.
- Has 4 * 10G client ports in the front side for each MPO port.
- Has dual power supply.

The benefits of using the breakout patch panel are as follows:

- Labels are assigned to each 10G client port and MPO port. 10G client ports are labeled 0-1 0-2 0-3 0-4, 1-1, 1-2, 1-3, 1-4, and so on. MPO ports are labeled 0, 1, 2, 3, and so on.
- Link status LED indication is provided to each 10G client port and MPO port.

The breakout patch panel can be connected to NCS 1002 using the following methods:

- The RJ45 Ethernet port, ETH2, available in the rear side of NCS 1002, is used to connect the breakout patch panel back-to-back with NCS 1002. This port is visible as MgmtEth0/RP0/CPU0/2 in IOS XR. The user must configure the ETH2 interface to bring up the back-to-back IP network.
- Management LAN, ETH0, can be used to connect breakout patch panel with NCS 1002. The user needs to manually bring up the patch panel using the serial port on the patch panel.

Configure Breakout Patch Panel

Connect Patch Panel Back-to-back with NCS 1002

Note Bring up the ETH2 interface in 198.51.100 network.

configure

interface *interface*

ipv4 *ipv4 address subnetmask*

no shut

exit

patch-panel

exit

commit

Example

The following is a sample to configure the breakout patch panel by connecting patch panel back-to-back with NCS 1002.

```
configure
interface MgmtEth0/RP0/CPU0/2
ipv4 address 198.51.100.4 255.255.255.0
no shut
exit
patch-panel
exit
commit
```

Connect Patch Panel with NCS 1002 Using Management LAN

The user needs to manually configure the ETH0 interface of the patch panel.

Issue the following commands from the patch panel.

sudo ifconfig eth0 ipaddress *ipaddress* **netmask** *ipaddress* **up**

sudo route add default gw *ipaddress*

Issue the following commands from NCS 1002.

patch-panel

ipv4 *ipv4 address*

exit

commit

Example

The following is a sample to configure the breakout patch panel using the management LAN.

From the patch panel:

```
sudo ifconfig eth0 192.0.2.19 netmask 255.255.255.0 up
sudo route add default gw 198.51.100.98
```

From NCS 1002:

```
patch-panel
ipv4 198.51.100.176
exit
commit
```

Display Patch Panel Events

show patch-panel events

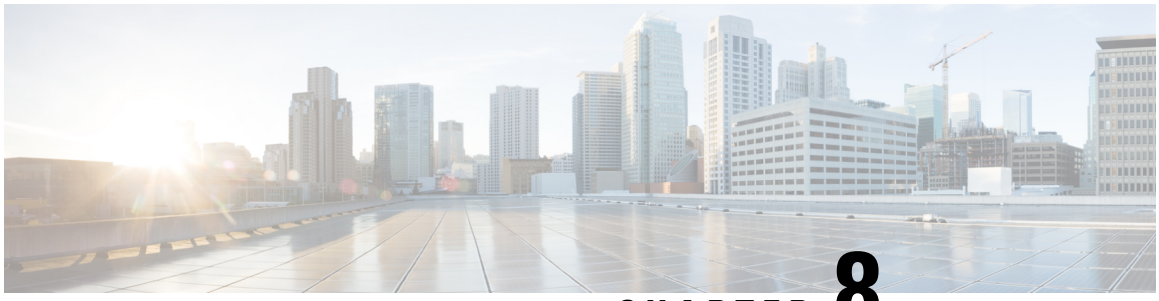
```
Mon Oct 24 12:07:19.963 UTC
{u'fimo_alarms_history_header': u'History of Alarms and Events'}
{u'fimo_alarms_history_help': u'(Time) (ID) (Type) (Message)'}
{u'events_800': u'(2016/09/17 18:37:58) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC2 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_799': u'(2016/09/17 18:37:58) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC3 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_798': u'(2016/09/17 18:37:57) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC4 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_797': u'(2016/09/17 18:37:57) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC5 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_796': u'(2016/09/17 18:37:57) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC8 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_795': u'(2016/09/17 18:37:57) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC9 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_794': u'(2016/09/17 18:37:56) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC10 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_793': u'(2016/09/17 18:37:56) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC11 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_792': u'(2016/09/17 18:37:56) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC12 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_791': u'(2016/09/17 18:37:55) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC13 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_790': u'(2016/09/17 18:37:55) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC14 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_789': u'(2016/09/17 18:37:55) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC15 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_788': u'(2016/09/17 18:37:55) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC16 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_787': u'(2016/09/17 18:37:54) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC17 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_786': u'(2016/09/17 18:37:54) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC18 data: port_led_color: off, port_led_mode:
```

```
 solid)'}
{u'events_785': u'(2016/09/17 18:37:54) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC19 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_784': u'(2016/09/17 18:37:54) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC20 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_783': u'(2016/09/17 18:37:53) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/LC1 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_782': u'(2016/09/17 18:37:53) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/MPO86 data: port_led_color: off, port_led_mode:
 solid)'}
{u'events_781': u'(2016/09/17 18:37:53) (4360) (Event) (Vars were changed; from IP:
198.51.100.125  table: port/b827eba9fb157000/MPO87 data: port_led_color: off, port_led_mode:
 solid)'}
```

The **patch-panel reset** command is used to reset the patch panel.

Alarms in Breakout Patch Panel

Two alarms, **NOT ABLE TO COMMUNICATE WITH PATCH-PANEL** and **PATCH-PANEL POWER REDUNDANCY LOST**, are raised for the breakout patch panel. For description and clearing procedures of these alarms, see the Alarm Troubleshooting chapter in the *Troubleshooting Guide for Cisco NCS 1000 Series*.



CHAPTER 8

Smart Licensing

This chapter describes Smart Licensing configuration on Cisco NCS 1002.

This chapter contains the following topics:

- Understanding Smart Licensing, on page 101
- Benefits of Smart Licensing, on page 104
- PIDs of NCS 1002, on page 104
- Software Entitlements and Smart Licenses of Cisco NCS 1002, on page 105
- Creating a Token, on page 106
- Configuring Smart Licensing, on page 106
- Verifying Smart Licensing Configuration, on page 107

Understanding Smart Licensing

Smart Licensing is a cloud-based approach to licensing. Smart Licensing simplifies the licensing experience across the enterprise making it easier to purchase, deploy, track, and renew Cisco Software. It provides visibility into license ownership and consumption through a single, simple user interface. The solution allows you to easily track the status of your license and software usage trends.

Smart Licensing helps you 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. Also, 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.
- **Reporting**: Through the portal, Smart Licensing offers an integrated view of the licenses you have purchased and what has been deployed in your network. You can use this data to make better purchasing 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.
- Licenses can be moved between product instances without license transfer. This greatly simplifies the reassignment of a software license as part of the Return Material Authorization (RMA) process.
- It provides a complete view of all the 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 you submit the request, it goes through a brief approval process. Access 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 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 tithing 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 that you can aggregate licenses into discrete bundles that are 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. After you access the default account, you may choose to transfer them to any other account, 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 that is associated with your enterprise account. Registration tokens can be valid 1–365 days.

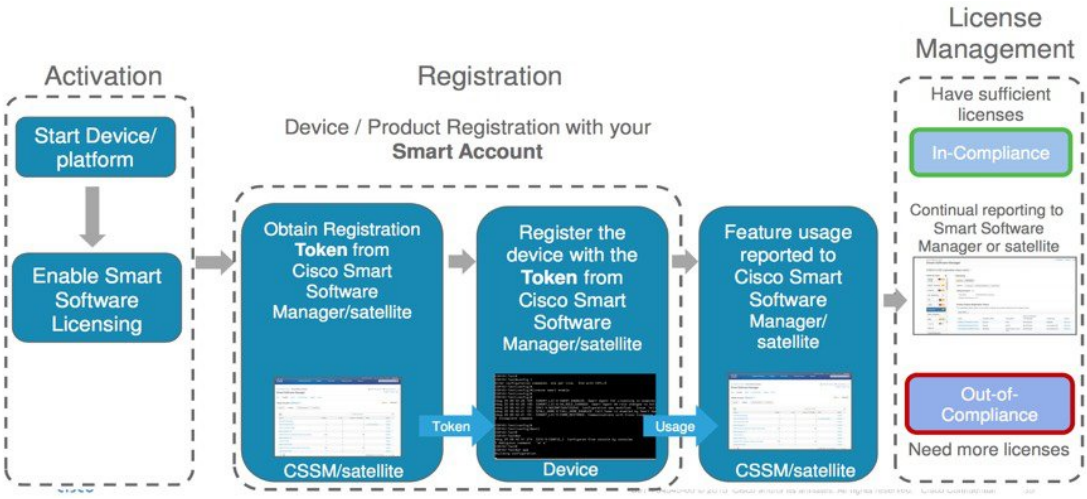
Product Instances

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.

Smart Licensing Work Flow

The following figure depicts a working model of smart licensing that involves a three-step procedure.

Figure 7: Smart Licensing Work Flow



1. **Setting up Smart Licensing**: You can place the order for Smart Licensing, to manage licenses on the 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 effectively pursue service and support contract

renewals. 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 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 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 must synchronize with Cisco SSM to reflect the latest license entitlements.

  For more information about the 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.

Benefits of Smart Licensing

- Licenses are not locked to perform configurations even if the license limit exceeds the paid license limit. You are notified with out-of-compliance notification to buy additional licenses when the license limit exceeds the paid license limit. This saves time with the ability to transfer licenses across the organization.
- Licenses can be pooled across the entire organization, enabling them to be reused across organizational boundaries.
- Provides software asset management information so that you can plan and track the licenses.

PIDs of NCS 1002

Cisco NCS 1002 has two PIDs:

- **Fully licensed PID (NCS1002-K9)**—This is a high cost PID. By using the fully licensed PID, you can configure and use the software without any explicit licensing.
- **Partially licensed PID (NCS1002-LIC-K9)**—This is a low cost PID and you have to additionally buy licenses to configure the software.

Software Entitlements and Smart Licenses of Cisco NCS 1002

Software entitlement is a system that consists of a license manager on Cisco NCS 1002 that manages licenses for various software and hardware features. The license manager parses and authenticates a license before accepting it.

Core features are available for use without any license. The following features are available on Cisco NCS 1002 only using licenses.

The following table lists the features and its corresponding entitlements that can be enabled on Cisco NCS 1002 using licenses:

Table 5: Software Entitlements of Cisco NCS 1002

Feature	Software Entitlement
NCS1K Smart License - one slice with 200G DWDM	L_NCS1K_200G_LIC
NCS1K Smart License - one slice with 200G/250G DWDM	L_NCS1K_250G_LIC
NCS1K Smart License - one slice with encryption	L_NCS1K_ENCR_LIC
(Only for R6.2.1 and R6.2.2) NCS1K Smart License - streaming telemetry	L-NCS1K-ST-LIC

Note You can view these software entitlements and their usage details in the Cisco Smart Software Manager portal.

There is one-to-one mapping mapping between the software entitlement and the smart license. For example, S-NCS1K-LIC-200G= license requested by the customer maps to the L_NCS1K_200G_LIC entitlement stored in the software.

Table 6: Smart Licenses of NCS 1002

License Requested	License Given	Configuartion Done
S-NCS1K-LIC-200G=	S-NCS1K-LIC-200G=	Slice with 200G trunk without encryption
S-NCS1K-LIC-250G=	S-NCS1K-LIC-200G= S-NCS1K-LIC-250G= (Additional 200G license will be given)	Slice with 250G or 200G trunk without encryption
		Slice with 200G trunk without encryption
S-NCS1K-LIC-ENCR=	S-NCS1K-LIC-ENCR=	One slice with encryption
(Only for R6.2.1 and R6.2.2) S-NCS1K-LIC-ST=	S-NCS1K-LIC-ST=	Telemetry configuration

Creating a Token

To create a new token using Cisco Smart Software Manager, perform the following tasks:

Step 1 Log into the Cisco Smart Software Manager.

Step 2 Click the **Inventory** tab, and select your virtual account from the **Virtual Account** drop-down list.

Step 3 From the **General** tab, choose **New Token**.

The **Create Registration Token** dialog appears.

Step 4 Enter the token description.

Step 5 Specify the number of days the token must be active.

Step 6 Check the **Allow export-controlled functionality on the products registered with this token** check box.

Step 7 Click **Create Token**.

Step 8 Copy the token and register NCS 1002 with the same token ID.

Configuring Smart Licensing

To configure smart licensing in Cisco NCS 1002, perform the following tasks:

Step 1 Configure the domain name server for the smart license server.

Example:

```
RP/0/RP0/CPU0:ios#configure
Sat Dec 15 15:25:14.385 IST
RP/0/RP0/CPU0:NCS1002(config)#domain name-server 203.0.113.247
```

Step 2 Setup the CiscoTAC-1 profile and destination address for Smart Call Home, using the following commands:

call-home

service active

contact smart-licensing

profile CiscoTAC-1

active

destination address http {http|https}://{FQDN}/its/service/oddce/services/DDCEService

destination transport-method http

Note FQDN must be either Cisco Smart Software Manager FQDN (tools.cisco.com) or Smart Licensing satellite server FQDN. You must configure the DNS server before setting-up the call-home destination address as FQDN. Use the **domain name-server {DNS server IP}** command to configure the DNS server on the device.

Example:

```
domain name-server 203.0.113.247
call-home
service active
contact smart-licensing
profile CiscoTAC-1
active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
```

Note **CiscoTAC-1** profile is the default profile for smart licensing and it must not be deleted.

Step 3 Configure the crypto ca Trust point profile, if CRL distribution point is not defined in the Satellite server certificate or if the device is not able to reach the host mentioned in the CRL distribution point.

Example:

```
RP/0/RP0/CPU0:ios(config)#crypto ca trustpoint Trustpool crl optional
```

Step 4 Create and copy the registration token ID using Cisco Smart Software Manager.

For more details about creating a token, see Creating a Token, on page 106.

Step 5 In the privileged EXEC mode, register the token ID in Cisco NCS 1002, using the following commands:

license smart register idtoken *token-ID*

The registration may fail if the token is invalid or there is communication failure between the device and the portal or satellite. If there is a communication failure, there is a wait time of 24 hours before the device attempts to register again. To force the registration, use the **license smart register idtoken** *token-ID* **force** command.

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.

ID certificates are renewed automatically after six months. In case, the renewal fails, the product instance goes into unidentified state. You can manually renew the ID certificate using the **license smart renew id** command.

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.

Verifying Smart Licensing Configuration

After enabling Smart Licensing, 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.

- **show license all**
- **show license status**
- **show license summary**

- **show license tech**
- **show license udi**
- **show license usage**
- **show license platform detail**
- **show tech-support smartlic**
- **show tech-support call-home**

The following table defines the available license authorization status in Cisco NCS1002:

Table 7: License Authorization Status

License Authorization Status	Description
Unconfigured	Smart Software Licensing is not configured.
Unidentified	Smart Software Licnensing is enabled but is not registered.
Registered	Device registration is completed and an ID certificate is received that will be used for future communication with the Cisco licensing authority.
Authorized	Registration is completed with a valid Smart Account and license consumption has begun. This indicates compliance.
Out of Compliance	Consumption exceeds available licenses in the Smart Account.
Authorization Expired	The device is unable to communicate with the Cisco Smart Software Manager for an extended period of time. This state occurs after 90 days of expiry. The device will attempt to contact the CSSM every hour in order to renew the authorization until the registration period expires.

Example 1:

The following example shows the sample output of **show license all** command.

```
RP/0/RP0/CPU0:ios#show license all
Fri Jan  6 01:33:24.230 UTC
Smart Licensing Status
======================
Smart Licensing is ENABLED
Registration:
 Status: REGISTERED
 Smart Account: BU Production Test
 Virtual Account: NCS1000  Initial
 Registration: SUCCEEDED on Thu Jan 05 2017 15:04:18 UTC
 Last Renewal Attempt: None
 Next Renewal Attempt: Tue Jul 04 2017 15:04:18 UTC
 Registration Expires: Fri Jan 05 2018 09:25:50 UTC
License Authorization:
 Status: AUTHORIZED on Thu Jan 05 2017 15:17:04 UTC
 Last Communication Attempt: SUCCEEDED on Thu Jan 05 2017 15:17:04 UTC
 Next Communication Attempt: Sat Feb 04 2017 15:17:04 UTC
 Communication Deadline: Fri Jan 05 2018 09:25:50 UTC
License Usage
=============
No licenses in use
Product Information
===================
```

```
UDI: SN:CAT1111B0KR,UUID:default-sdr
Agent Version=============Smart Agent for Licensing: 2.2.0_rel/17RP/0/RP0/CPU0:ios#
```

Example 2:

The following example shows the sample output of **show license platform detail** command. The output displays telemetry entry only for R6.2.1 and R6.2.2.

```
RP/0/RP0/CPU0:ios#show license platform detail
Fri Jan 20 12:09:30.729 UTC
Current state:    REGISTERED
Collection: LAST: Fri Jan 20 12:03:13 2017
            NEXT: Fri Jan 20 13:03:13 2017
Reporting:  LAST: Fri Jan 20 12:03:13 2017
            NEXT: Sat Jan 21 12:03:13 2017
Parameters: Collection interval:          60 minute(s)
            Reporting  interval:        1440 minute(s)
            Throughput gauge:        1000000 Kbps
================================================
Feature/Area 'sys_features'
   Name:  sys_features
   DLL:   libplat_sl_plugin_sys_features.so
   Flags: CONFIG
   # CLI: 1
   Entitlements (total 1):
   [ 0] Name:  NCS1K Smart License - streaming telemetry
        Token:
regid.2017-01.com.cisco.L-NCS1K-ST-LIC-,1.0_6222b080-6651-4611-a725-fc84b647d614
        Count: Last reported:    1
               Next report:      0
================================================
Feature/Area 'system'
   Name:  System
   DLL:   libplat_sl_plugin_system.so
   Flags: CONFIG
   # CLI: 3
   Entitlements (total 3):
   [ 0] Name:  NCS1K Smart License - one slice with 200G DWDM
        Token:
regid.2017-01.com.cisco.L-NCS1K-200G-LIC,1.0_b03ac261-7397-4a66-b1e2-affa324ac518
        Count: Last reported:    0
               Next report:      0
   [ 1] Name:  NCS1K Smart License - one slice with 200G/250G DWDM
        Token:
regid.2017-01.com.cisco.L-NCS1K-250G-LIC,1.0_c0520a76-f3f9-4773-b841-60fadfa70e4e
        Count: Last reported:    0
               Next report:      0
   [ 2] Name:  NCS1K Smart License - one slice with encryption
        Token:
regid.2017-01.com.cisco.L-NCS1K-ENCR-LIC-,1.0_18fbcf09-68a5-4853-9534-cdbcad8dc918
        Count: Last reported:    0
               Next report:      0
```

Example 3:

The following example shows the sample output of **show license summary** command.

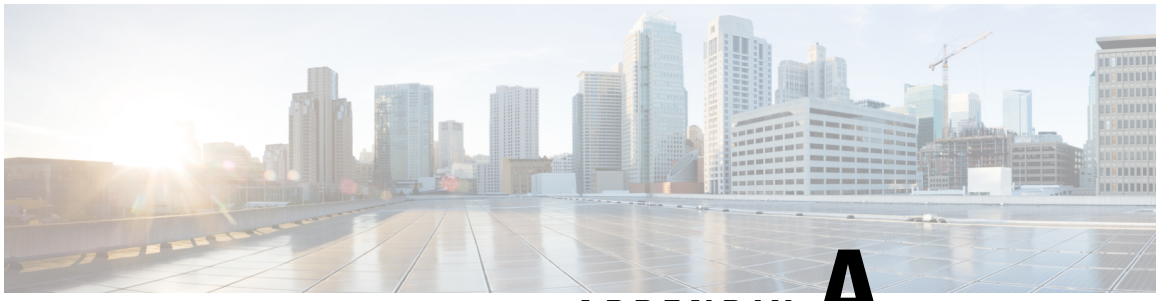
```
RP/0/RP0/CPU0:ios#show license summary
Thu Feb  2 23:10:46.723 UTC
Smart Licensing is ENABLED
Registration:
  Status: REGISTERED
  Smart Account: BU Production Test
```

```
  Virtual Account: NCS1000
  Last Renewal Attempt: None
  Next Renewal Attempt: Tue Aug 01 2017 23:09:00 UTC
License Authorization:
  Status: AUTHORIZED on Thu Feb 02 2017 23:09:12 UTC
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Thu Feb 02 2017 23:10:53 UTC
License Usage:
  License             Entitlement tag          Count  Status
  -----------------------------------------------------------------
                      (L-NCS1K-200G-LIC)           2   PENDING
                      (L-NCS1K-250G-LIC)           1   PENDING
                      (L-NCS1K-ENCR-LIC-)          1   PENDING
```

Example 4:

The following example shows the sample output of **show license usage** command.

```
RP/0/RP0/CPU0:ios#show license usage
Fri Feb  3 21:08:24.097 UTC
License Authorization:
  Status: No Licenses in Use
RP/0/RP0/CPU0:ios#
RP/0/RP0/CPU0:ios#show license trace ?
  all       Show tracing for both Smart Licensing and client(cisco-support)
  client    Show tracing for the agent client code(cisco-support)
  smartlic  Show tracing for the Smart Licensing Code(cisco-support)
```



APPENDIX A

Configuring SNMP

The following MIBs are supported in NCS 1002.

- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-ENTITY-REDUNDANCY-MIB
- CISCO-SYSTEM-MIB
- CISCO-ENTITY-ASSET-MIB
- EVENT-MIB
- DISMAN-EXPRESSION-MIB
- CISCO-FTP-CLIENT-MIB
- NOTIFICATION-LOG-MIB
- CISCO-RF-MIB
- RADIUS-AUTH-CLIENT-MIB
- RADIUS-ACC-CLIENT-MIB
- IEEE8023-LAG-MIB
- CISCO-TCP-MIB
- UDP-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CONTEXT-MAPPING-MIB
- CISCO-OTN-IF-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-PROCESS-MIB
- CISCO-SYSLOG-MIB
- ENTITY-MIB

- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-IF-EXTENSION-MIB
- RMON-MIB
- CISCO-OPTICAL-MIB
- CISCO-ENTITY-SENSOR-MIB
- LLDP-MIB
- IEEE8021-SECY-MIB (only SNMP read-only operations are supported for this MIB). For more information, see http://www.ieee802.org/1/files/public/MIBs/IEEE8021-SECY-MIB-200601100000Z.mib.

The following table provides more information about SNMP MIBs and the documentation links.

Task	Link
Determine the MIB definitions	SNMP Object Navigator
Configure SNMP	Configure SNMP
Understand the SNMP best practices regarding the recommended order of SNMP query, maximum cache hit, and SNMP retry and timeout recommendation	SNMP Best Practices

snmp-server community must be configured as SystemOwner for admin-plane parameters to appear to entity mib. The parameters of fans and power supply units are examples of admin-plane parameters.