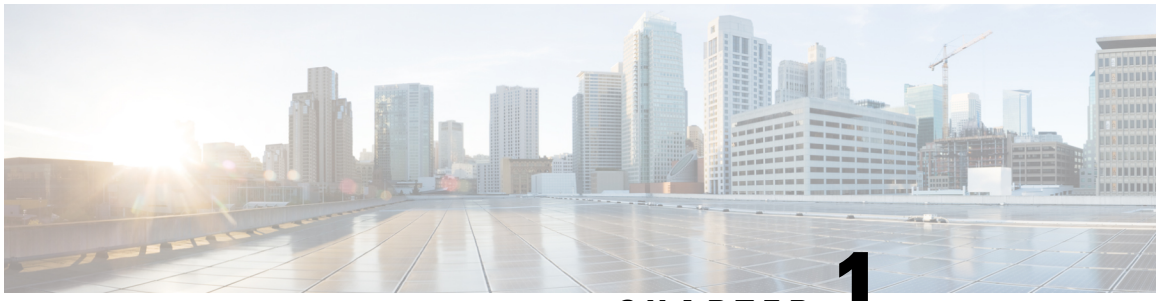


Command Reference for Cisco NCS 1004

First Published: 2024-06-14

Last Modified: 2025-09-16

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



CHAPTER 1

List of Commands

This guide describes the commands supported in NCS 1004.

- aaa authentication login, on page 4
- aaa authorization, on page 5
- aaa authorization (System Admin-VM), on page 6
- active, on page 7
- address, on page 8
- ains-soak (OTN-XP Card), on page 9
- automatic-in-service (OTN-XP Card), on page 9
- authentication, on page 10
- cipher-suite, on page 11
- controller coherentDSP, on page 12
- controller HundredGigECtrlr, on page 15
- controller FourHundredGigECtrlr, on page 17
- controller TenGigECtrlr (OTN-XP Card), on page 18
- controller odu2e (OTN-XP Card), on page 19
- controller ODU4, on page 20
- controller ODUC4, on page 21
- controller odu-group-mp, on page 23
- controller OTU (OTN-XP Card), on page 24
- controller optics, on page 25
- crypto ca authenticate, on page 29
- crypto ca enroll, on page 30
- crypto ca trustpoint, on page 32
- crypto key generate dsa, on page 33
- crypto key generate ecdsa, on page 34
- crypto key generate ed25519, on page 36
- crypto key generate rsa, on page 37
- crypto key import authentication rsa, on page 39
- crypto key zeroize ed25519, on page 39
- crypto key zeroize rsa, on page 40
- destination address, on page 41
- destination ipv4 unicast, on page 42
- destination transport-method, on page 42

- dh, on page 43
- dwdm-carrier, on page 44
- encryption, on page 45
- enrollment retry count, on page 46
- enrollment retry period, on page 47
- enrollment terminal, on page 48
- enrollment url, on page 48
- fault-profile, on page 50
- fault-profile apply, on page 51
- gmpls optical-uni, on page 52
- http client connection, on page 52
- http client response, on page 53
- http client ssl, on page 54
- http client secure-verify-host, on page 54
- http client secure-verify-peer, on page 55
- http client source interface, on page 56
- http client tcp-window-scale, on page 57
- http client version, on page 57
- http client vrf , on page 58
- http-proxy, on page 59
- hw-module, on page 59
- hw-module (OTN-XP Card), on page 64
- ikev2 policy, on page 67
- ikev2 profile, on page 68
- ikev2 proposal, on page 69
- integrity, on page 70
- interface gcc0, on page 71
- interface gcc2, on page 71
- ipcc routed, on page 72
- ipv4 access-group, on page 73
- ipv6 access-group, on page 74
- key config-key password-encryption, on page 75
- keyring, on page 75
- lc-module (OTN-XP Card), on page 78
- license smart register, on page 79
- license smart renew , on page 79
- license smart deregister, on page 80
- lifetime, on page 81
- link-id ipv4 unicast, on page 82
- linux security audit, on page 82
- lmp, on page 84
- match address local, on page 84
- match identity remote address, on page 85
- neighbor interface-id unnumbered, on page 86
- neighbor link-id ipv4 unicast, on page 87
- neighbor, on page 87

- nvgen default-sanitize, on page 88
- otnsec policy, on page 89
- password6 aes encryption, on page 89
- path-option, on page 90
- peer, on page 91
- pki trustpoint, on page 92
- pm, on page 92
- prf, on page 97
- protecting-controller, on page 98
- protection-attributes connection-mode, on page 99
- protection-attributes protection-mode, on page 100
- protection-attributes protection-type, on page 101
- protection-attributes timers, on page 101
- protection-switching, on page 102
- query url, on page 103
- router-id ipv4 unicast, on page 104
- rsakeypair, on page 105
- sftp-password (trustpoint), on page 105
- sftp-username (trustpoint), on page 106
- show configuration commit changes, on page 107
- show controllers [odu-group-mp], on page 110
- show crypto ca certificates, on page 112
- show crypto key mypubkey ed25519, on page 114
- show crypto key mypubkey rsa, on page 115
- show linux security audit, on page 116
- sak-rekey-interval, on page 117
- security-policy, on page 117
- session-id, on page 118
- show alarms, on page 119
- show controllers, on page 121
- show access-lists ipv4, on page 137
- show access-lists ipv6, on page 138
- show environment, on page 139
- show hw-module, on page 142
- show inventory, on page 145
- show lc-module (OTN-XP Card), on page 151
- show led, on page 152
- show platform, on page 153
- show tcp dump-file, on page 155
- show type6, on page 156
- signalling refresh out-of-band interval, on page 157
- signalling refresh out-of-band missed, on page 158
- sks profile, on page 158
- split-client-port-mapping, on page 159
- subject-name (trustpoint), on page 160
- ssh server timeout, on page 161

- tcp dump-file convert, on page 162
- tunnel-id, on page 163
- tunnel-properties, on page 164
- working-controller, on page 164

aaa authentication login

To configure authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode.

aaa authentication login { default | *list-name* **}** *method-list*

Syntax Description

login	Sets authentication for login.
default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
list-name	Character string used to name the authentication method list.
method-list	Method used to enable AAA system accounting. Method list types are entered in the preferred sequence. The value is one of the following options: • **group tacacs+** — Specifies a method list that uses the list of all configured TACACS+ servers for authentication. • **group radius** — Specifies a method list that uses the list of all configured RADIUS servers for authentication. • **group** *named-group* — Specifies a named subset of TACACS+ or RADIUS servers for authentication. • **local** — Specifies a local username or password database for authentication. • **line** — Specifies a line password or user group for authentication.

Command Default

No authentication is performed.

Command Modes

Global configuration

Command History

Release	Modification
R7.0.1	This command was introduced.

Example

The following example shows how to specify the default method list for authentication, and also enable authentication.

```
configure
aaa authentication login default group tacacs+
```

```
exit
commit
```

aaa authorization

To create a method list for authorization, use the **aaa authorization** command in global configuration mode.

aaa authorization {exec | nacm} { default | *list-name* **} {none | local | group tacacs+ | group radius | group** *group-name* **}**

Syntax Description

exec	Configures authorization for an interactive (EXEC) session.
nacm	Enables the NACM (NETCONF Access Control Model) functionality.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
none	Uses no authorization. If you specify **none**, no subsequent authorization method is attempted.
local	Uses local authorization. This method of authorization is not available for command authorization.
group tacacs+	Uses the list of all configured TACACS+ servers for authorization.
group radius	Uses the list of all configured RADIUS servers for authorization. This method of authorization is not available for command authorization.
group *group-name*	Specifies a named subset of TACACS+ or RADIUS servers for authorization.

Command Default

Authorization is disabled for all actions (equivalent to the method none keyword).

Command Modes

Global configuration

Command History

Release	Modification
R7.0.1	This command was introduced.

Example

The following example shows how to define the network authorization method list named listname1, which specifies that TACACS+ authorization is used.

```
configure
aaa authorization exec listname1 group tacacs+
exit
commit
```

aaa authorization (System Admin-VM)

To create command rules and data rules for user authorization, use the **aaa authorization** command in System Admin Config mode. To delete the command rules and data rules, use the **no** form of this command.

aaa authorization { **cmdrules cmdrule** { *integer* | **range** *integer* } [**action** *action-type* | **command** *cmd-name* | **context** *context-name* | **group** *group-name* | **ops** *ops-type*] | **commands group** { **none** | **tacacs** } | **datarules datarule** { *integer* | **range** *integer* } [**action** *action-type* | **context** *context-name* | **group** *group-name* | **keypath** *keypath-name* | **namespace** *namespace-string* | **ops** *ops-type*] }

Syntax Description

cmdrules	Configures command rules.
cmdrule *integer*	Specifies the command rule number.
range *integer*	Specifies the range of the command rules or data rules to be configured.
action *action-type*	Specifies whether users are permitted or not allowed to perform the operation specified for the **action-type** keyword. The **action-type** specifies the action type for the command rule or data rule. Available options are: **accept**, **accept_log** and **reject**.
command *cmd-name*	Specifies the command to which the command rule applies. The command must be entered within double-quotes. Example, **get**.
context *context-name*	Specifies to which type of connection the command rule or data rule applies. The connection type can be netconf, cli, or xml.
group *group-name*	Specifies the group to which the command rule or data rule applies. Example, **admin-r**.
ops *ops-type*	Specifies whether the user has read, execute, or read and execute permissions for the command. Available options for command rules are: **r**, rx, and **x**. To know the available options for data rules, use a **?** after the **ops** keyword.
commands group	Sets the command authorization lists for server groups. Available options are **none** that specifies no authorization and **tacacs** that specifies use of the list of all tacacs+ hosts.

Command Default

None

Command Modes

System Admin Config mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

From Cisco IOS XR Software Release 7.3.2, the system internally maps the users configured on the XR VM to System Admin VM of the router, based on the task table of the user on the XR VM. With this feature, NETCONF and gRPC users can access the admin-related information on the router even if their user profiles do not exist on System Admin VM. For a sample configuration, see the example section.

This example shows how to create a command rule:

```
Router#admin
sysadmin-vm:0_RP0#configure
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 6
sysadmin-vm:0_RP0(config-cmdrule-6)#context netconf
sysadmin-vm:0_RP0(config-cmdrule-6)#command get
sysadmin-vm:0_RP0(config-cmdrule-6)#group admin-r
sysadmin-vm:0_RP0(config-cmdrule-6)#ops rx
sysadmin-vm:0_RP0(config-cmdrule-6)#action accept
sysadmin-vm:0_RP0(config)#commit
```

active

To enable a Call Home profile, use the **active** command in the call home profile configuration mode.

active

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Call home profile configuration mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

You must enable a profile using the **active** command so that call home messages can be triggered.

The following example shows how to activate a profile.

```
domain name-server 192.0.2.6
call-home
service active
contact smart-licensing
profile CiscoTAC-1
active
```

address

To configure the IP address of the peer node during keyring configuration, use the **address** command in keyring configuration mode.

address { *ipv4-address* [*subnet-mask*] }

Syntax Description

ipv4-address	IP address of the peer node.
subnet-mask	Subnet mask address.

Command Default

None

Command Modes

Keyring configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Example

The following is a sample in which an OTNSec policy is configured.

```
RP/0/RP0/CPU0:ios#conf
Thu Mar  7 19:33:14.594 UTC
RP/0/RP0/CPU0:ios(config)#keyring kyr1
RP/0/RP0/CPU0:ios(config-keyring-kyr1)#peer peer1
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#pre-shared-key key1|clear
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#commit
Thu Mar  7 19:54:33.314 UTC
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#exit
RP/0/RP0/CPU0:ios(config-keyring-kyr1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show keyring kyr1
Thu Mar  7 19:58:07.135 UTC

Keyring Name                          : kyr1
================================================================================
Total Peers                           : 1
--------------------------------------------------------------------------------
   Peer Name                          : peer1
   IP Address                         : 10.0.0.1
   Subnet Mask                        : 255.255.255.0
   Local PSK                          : Configured
   Remote PSK                         : Configured
```

ains-soak (OTN-XP Card)

To configure the default AINS settings for all controllers on the OTN-XP card, use the **ains-soak** command in the IOS XR configuration mode. The configuration is applied to any OTN-XP line card that is installed in the Cisco NCS 1004.

ains-soak hours *hours* **minutes** *minutes*

Syntax Description

ains-soak hours *hours* **minutes** *minutes*	Specifies the AINS configuration in hours and minutes.

Command Default

None

Command Modes

Cisco IOS XR Configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Example

The following is a sample in which all the controllers on the OTN-XP card are configured with AINS with soak time period specified to be two minutes.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#ains-soak hours 0 minutes 2
RP/0/RP0/CPU0:ios(config)#commit
```

automatic-in-service (OTN-XP Card)

To override the default AINS settings on a specific controller on the OTN-XP card, use the **automatic-in-service** command.

Note This configuration does not persist after a RP reload operation.

automatic-in-service controller optics *R/S/I/P* **hours** *hours* **minutes** *minutes*

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port of the optics controller.
hours **minutes** *minutes*	Specifies the AINS configuration in hours and minutes.

Command Default None

Command Modes None

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Example

The following is a sample in which the optics controller on the OTN-XP card is configured with a soak time period of 45 minutes.

```
RP/0/RP0/CPU0:ios#automatic-in-service controller optics 0/1/0/0 hours 0 minutes 45
```

authentication

To configure the local or remote authentication method for the IKEv2 profile, use the **authentication** command in IKEv2 profile configuration mode.

Note You can specify only one local authentication method but multiple remote authentication methods.

authentication {local pre-share | rsa-signature} {remote pre-share | rsa-signature}

Syntax Description

pre-share	Specifies the preshared key as the authentication method.
rsa-signature	Specifies RSA signature as the authentication method.

Command Default None

Command Modes IKEv2 profile configuration

Command History

Release	Modification
R7.2.1	This command was introduced.

Example

The following example shows how to specify the authentication mode in the IKEv2 profile.

```
RP/0/RP0/CPU0:ios#configure
Thu May 7 16:22:33.804 IST
RP/0/RP0/CPU0:ios(config)#ikev2 profile IP1
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#match identity remote address 10.1.1.2
255.255.255.255
```

```
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#pki trustpoint myca
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#lifetime 120
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#authentication local rsa-signature
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#authentication remote rsa-signature
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#commit
```

cipher-suite

To specify the encryption algorithm for an OTNSec policy, use the **cipher-suite** command in the OTNSec policy configuration mode.

cipher-suite *encryption-algorithm-type*

Syntax Description

encryption-algorithm-type	Encryption algorithm type. AES-GCM-256 is used.

Command Default

None

Command Modes

OTNSec policy configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Example

The following is a sample in which an OTNSec policy is configured.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 11 15:16:58.417 UTC
RP/0/RP0/CPU0:ios(config)#otnsec policy otnsec-policy1
RP/0/RP0/CPU0:ios(config-otnsec-policy)#cipher-suite AES-GCM-256
RP/0/RP0/CPU0:ios(config-otnsec-policy)#security-policy must-secure
RP/0/RP0/CPU0:ios(config-otnsec-policy)#sak-rekey-interval 120
RP/0/RP0/CPU0:ios(config-otnsec-policy)#commit
```

The following is a sample of an OTNSec policy.

```
RP/0/RP0/CPU0:ios#show run otnsec policy otnsec-policy1
Tue Mar 12 11:14:03.591 UTC
otnsec policy otnsec-policy1
 cipher-suite AES-GCM-256
 security-policy must-secure
 sak-rekey-interval 120
!
```

controller coherentDSP

To configure the coherent DSP controller, use the **controller coherentDSP** command in the Coherent DSP controller configuration mode.

controller coherentDSP *R/S/I/P* [**description**] | [**fec** *fec-value*] | [**pm** { **30-sec |15-min | 24-hour** } { **fec | otn** } { **report | threshold** } *value*] | [**perf-mon** { **enable** | **disable** }] | [**loopback internal**] | [**secondary-admin-state** { **maintenance | normal** }] | [**shutdown**] | [**tti** { **sent | expected** } { **ascii | hex** } *tti-string*] [**gcc0**] [**flexo** { **gid** *gid-no* **| iid** *iid-no* }]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port of the coherent DSP controller.
description *description*	Description of the coherent DSP controller.
fec *fec-value*	Configures the FEC on the controller. The supported options on the 1.2T line card are StandardSD15 and StandardSD27. From Release 7.2.1 onwards, the supported options on the OTN XP card are EnhancedSD15 and EnhancedSD27. From Release 7.3.1 onwards, OFEC is supported on the OTN XP card.
pm {**30-sec |15-min	24-hour**} {**fec	otn**} {**report	threshold**} *value*	Configures performance monitoring parameters for 30 second, 15 minute, or 24-hour intervals. The **fec** keyword configures FEC PM data in 30 second, 15 minute, or 24-hour intervals. The **otn** keyword configures OTN PM data in 30 second, 15 minute, or 24-hour intervals. The **report** keyword configures TCA reporting status. The **threshold** keyword configures threshold values on PM parameters.
perf-mon { **enable**	**disable** }	Enables or disables performance monitoring.
loopback internal	Configures the internal loopback mode on the controller. For the 1.2T line card, internal and line loopbacks are supported on the Ethernet controllers whereas only internal loopback is supported on the CoherentDSP controllers.
secondary-admin-state	Configures the administrative state of the controller. The values are maintenance or normal.
shutdown	Disables the configuration of the controller.
**tti sent {ascii	hex}** *tti-string*	Configures the Trail Trace Identifier (TTI) ASCII or hex string to be sent. From Release 7.3.2 onwards, TTI strings such as SAPI, DAPI, and operator inputs are supported.

tti expected {ascii | hex} *tti-string*	Configures the expected TTI ASCII or hex string. The OTUK-TIM alarm is raised if the received TTI string does not match the expected TTI string. From Release 7.3.2 onwards, TTI strings such as SAPI, DAPI, and operator inputs are supported.
gcc0	Enables the GCC0 interface.
flexo { **gid***gid-no* **| iid***iid-no* }]	Configures FlexO group identification (GID) and FlexO instance identification (IID) on the controller. The range of the **gid** *gid-no* is 1–1,048,576. The range of the **iid** *iid-no* is 1–254.

Command Default

None

Command Modes

Coherent DSP controller configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.1.1	**gcc0** keyword was added.
Release 7.2.1	The following FEC options for the OTN-XP card were added. • ***EnhancedSD15*** • ***EnhancedSD27***
Release 7.3.1	The following FEC options for the OTN-XP card were added. • ***OFEC***
Release 7.3.1	The **flexo** { **gid***gid-no* **| iid***iid-no* }] keyword and options were added.
Release 7.3.2	TTI strings such as SAPI, DAPI, and operator inputs were supported.

Example

The following is a sample in which performance monitoring parameters of Coherent DSP controller is configured in 30-second intervals.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/0/1/1 pm 30-sec fec threshold post-fec-ber
 max OE-15
RP/0/RP0/CPU0:ios(config)#commit
```

The following example shows how to configure TTI on a coherentDSP controller with the sent and expected strings set to the same ASCII string. The state of the controller is up.

```
RP/0/RP0/CPU0:ios#configure
```

```
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/1/0/1 tti sent ascii 1234
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/1/0/1 tti expected ascii 1234
RP/0/RP0/CPU0:ios(config)#commit
```

The following example shows how to configure TTI on a coherentDSP controller with the sent and expected strings set to different ASCII strings. The state of the controller goes down and the OTUK-TIM alarm is raised.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/1/0/1 tti sent ascii 1234
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/1/0/1 tti expected ascii 5678
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample to enable the GCC0 interface.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller CoherentDSP0/0/0/0
RP/0/RP0/CPU0:ios(config-CoDSP)#gcc0
RP/0/RP0/CPU0:ios(config-CoDSP)#commit
RP/0/RP0/CPU0:ios(config-CoDSP)#exit
```

The following is a sample to configure FEC with the EnhancedSD15 option on the CoherentDSP controller of the OTN-XP card:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/0/0/0
RP/0/RP0/CPU0:ios(config-CoDSP)#fec EnhancedSD15
Tue Feb 25 11:25:52.670 UTC
WARNING! Changing FEC mode can impact traffic
RP/0/RP0/CPU0:ios(config-CoDSP)#commit
```

The following is a sample to configure with the O-FEC option on the CoherentDSP controller of the OTN-XP card:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/0/0/0
RP/0/RP0/CPU0:ios(config-CoDSP)#fec OFEC
Tue Feb 25 11:25:52.670 UTC
WARNING! Changing FEC mode can impact traffic
RP/0/RP0/CPU0:ios(config-CoDSP)#commit
```

The following is a sample to configure flexO GID and IID on the CoherentDSP controller of the OTN-XP card:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller coherentDSP0/2/0/12
RP/0/RP0/CPU0:ios(config-CoDSP)#flexo
RP/0/RP0/CPU0:ios(config-CoDSP)#gid 2 iid 5,6,7,8
RP/0/RP0/CPU0:ios(config-CoDSP)#commit
```

The following sample displays how to configure loopback on a coherent DSP controller ports on the OTN-XP in inverse muxponder configuration mode.

```
Thu Sep 30 14:16:04.678 UTC
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/2/0/12
RP/0/RP0/CPU0:ios(config-CoDSP)#secondary-admin-state maintenance
RP/0/RP0/CPU0:ios(config-CoDSP)#loopback internal
RP/0/RP0/CPU0:ios(config-CoDSP)#commit
Thu Sep 30 14:16:19.594 UTC
```

```
RP/0/RP0/CPU0:ios(config-CoDSP)#controller coherentDSP 0/2/0/13
RP/0/RP0/CPU0:ios(config-CoDSP)#secondary-admin-state maintenance
RP/0/RP0/CPU0:ios(config-CoDSP)#loopback internal
RP/0/RP0/CPU0:ios(config-CoDSP)#commit
```

The following sample displays how to configure TTI on a coherent DSP controller port 12 on the OTN-XP in inverse muxponder configuration mode.

```
RP/0/RP0/CPU0:ios#configure
Thu Sep 30 14:18:13.288 UTC
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/2/0/12
RP/0/RP0/CPU0:ios(config-CoDSP)#tti sent sapi ascii cisco
RP/0/RP0/CPU0:ios(config-CoDSP)#commit
```

controller HundredGigECtrlr

To configure the Ethernet controller, use the **controller HundredGigECtrlr** command in the Ethernet controller configuration mode.

controller HundredGigECtrlr *R/S/I/P* [**pm** { **30-sec |15-min | 24-hour** } { **ether** } { **report | threshold** } *value*] | [**perf-mon disable**] | [**loopback** { **internal** | **line** }] | [**sec-admin-state** *maintenance*] | [**shutdown**] | [**laser-squelch**] | [**fec** { **none** | **standard** }] | [**holdoff-time trunk-fault** *timevalue*] **insert-idle ingress** **insert-idle egress**

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port of the Ethernet controller.
pm { **30-sec | 15-min | 24-hour** }	Configures performance monitoring parameters for 30 second, 15 minutes, or 24 hour intervals.
ether	Configures Ethernet PM data in 30 second, 15 minute or 24 hour intervals.
report	Configures TCA reporting status.
threshold	Configures threshold on Ethernet controller parameters.
perf-mon disable	Disables performance monitoring.
loopback [internal | line]	Configures the internal or line loopback mode on the Ethernet controller. For the 1.2T line card, internal and line loopbacks are supported on the ethernet controllers whereas only internal loopbacks are supported on the CoherentDSP controllers.
sec-admin-state *maintenance*	Configures the administrative state of the controller indicating that the controller is under maintenance.
shutdown	Disables the configuration of the controller.
laser-squelch	Enables laser squelching so that laser is brought down in the event of trunk faults (LOF, LOS) and a SQUELCHED alarm is raised.

fec { **none** | **standard** }	Disables FEC or enables standard (Reed-Solomon) FEC.
holdoff-time trunk-fault *timevalue*	When a fault occurs on the trunk port, the user can hold the propagation of Local Fault using this parameter. The range of *timevalue* is 0 to 3000 ms.
insert-idle ingress	Enables idle frames insertion in the ingress direction.
insert-idle egress	Enables idle frames insertion in the egress direction.

Command Default

None

Command Modes

Ethernet controller configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.5.2	**insert-idle ingress** and **insert-idle egress** keywords were added.

Example

The following example shows how to configure the performance monitoring parameters of the Ethernet controller in 15 minute intervals.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 pm 15-min pcs report bip
enable
```

The following example shows how to configure the internal loopback.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 secondary-admin-state
maintenance
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 loopback internal
RP/0/RP0/CPU0:ios(config)#commit
```

The following example enables IDLE hold off timer in Ethernet controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 holdoff-time trunk-fault
3000
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample where laser quelching is enabled on the Ethernet controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 laser-squelch
RP/0/RP0/CPU0:ios(config)#commit
```

controller FourHundredGigECtrlr

To configure the Ethernet controller, use the **controller FourHundredGigECtrlr** command in the Ethernet controller configuration mode.

controller FourHundredGigECtrlr *R/S/I/P* [**pm** { **30-sec |15-min | 24-hour** } { **ether** } { **report | threshold** } *value*] | [**perf-mon disable**] | [**loopback** { **internal** | **line** }] | [**sec-admin-state** *maintenance*] | [**shutdown**] | [**laser-squelch**] | [**fec** { **none** | **standard** }] | [**holdoff-time trunk-fault** *timevalue*] **insert-idle ingress** **insert-idle egress**

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port of the Ethernet controller.
pm { **30-sec | 15-min | 24-hour** }	Configures performance monitoring parameters for 30 second, 15 minutes, or 24 hour intervals.
ether	Configures Ethernet PM data in 30 second, 15 minute or 24 hour intervals.
report	Configures TCA reporting status.
threshold	Configures threshold on Ethernet controller parameters.
perf-mon disable	Disables performance monitoring.
loopback [internal | line]	Configures the internal or line loopback mode on the Ethernet controller. For the 1.2T line card, internal and line loopbacks are supported on the ethernet controllers whereas only internal loopbacks are supported on the CoherentDSP controllers.
sec-admin-state *maintenance*	Configures the administrative state of the controller indicating that the controller is under maintenance.
shutdown	Disables the configuration of the controller.
laser-squelch	Enables laser squelching so that laser is brought down in the event of trunk faults (LOF, LOS) and a SQUELCHED alarm is raised.
fec { **none** | **standard** }	Disables FEC or enables standard (Reed-Solomon) FEC.
holdoff-time trunk-fault *timevalue*	When a fault occurs on the trunk port, the user can hold the propagation of Local Fault using this parameter. The range of *timevalue* is 0 to 3000 ms.
insert-idle ingress	Enables idle frames insertion in the ingress direction.
insert-idle egress	Enables idle frames insertion in the egress direction.

Command Default

None

Command Modes

Ethernet controller configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.
Release 7.5.2	**insert-idle ingress** and **insert-idle egress** keywords were added.

Example

The following example shows how to configure the performance monitoring parameters of the Ethernet controller in 15 minute intervals.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 pm 15-min pcs report bip
enable
```

The following example shows how to configure the internal loopback.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 secondary-admin-state
maintenance
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 loopback internal
RP/0/RP0/CPU0:ios(config)#commit
```

The following example enables IDLE hold off timer in Ethernet controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 holdoff-time trunk-fault
3000
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample where laser quelching is enabled on the Ethernet controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/1/0/10 laser-squelch
RP/0/RP0/CPU0:ios(config)#commit
```

controller TenGigECtrlr (OTN-XP Card)

To configure the Ethernet controller, use the **controller TenGigECtrlr** command in the Ethernet controller configuration mode.

From R7.2.1 onwards, the TenGig Ethernet controller configuration is supported on the OTN-XP card.

controller TenGigECtrlr *R/S/I/P/L* [**pm** { **30-sec |15-min | 24-hour** } **perf-mon disable**] | [**loopback** { **internal** | **line** }] | [**sec-admin-state** *maintenance*] | [**shutdown**] | [**laser-squelch**] | [**holdoff-time trunk-fault** *timevalue*]

Syntax Description

R/S/I/P/L	Rack/Slot/Instance/Port/Lane of the Ethernet controller.
pm {**30-sec | 15-min | 24-hour** }	Configures performance monitoring parameters for 30 second, 15 minutes, or 24 hour intervals.

perf-mon disable	Disables performance monitoring.
loopback [internal | line]	Configures the internal or line loopback mode on the Ethernet controller.
sec-admin-state *maintenance*	Configures the administrative state of the controller indicating that the controller is under maintenance.
shutdown	Disables the configuration of the controller.
laser-squelch	Enables laser squelching so that laser is brought down in the event of trunk faults and a SQUELCHED alarm is raised.
holdoff-time trunk-fault *timevalue*	When a fault occurs on the trunk port, the user can hold the propagation of Local Fault using this parameter. The range of *timevalue* is 0 to 3000 ms.

Command Default

None

Command Modes

Ethernet controller configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Examples

The following example shows how to configure the internal loopback.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller TenGigECtrlr 0/0/0/4/1secondary-admin-state maintenance
RP/0/RP0/CPU0:ios(config)#controller TenGigECtrlr 0/0/0/4/1 loopback internal
RP/0/RP0/CPU0:ios(config)#commit
```

The following example enables IDLE hold off timer in Ethernet controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller TenGigECtrlr 0/0/0/4/1 holdoff-time trunk-fault 3000
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample where laser quelching is enabled on the Ethernet controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller TenGigECtrlr 0/0/0/4/1 laser-squelch
RP/0/RP0/CPU0:ios(config)#commit
```

controller odu2e (OTN-XP Card)

To configure the ODU2e controller, use the **controller odu2e** command in the configuration mode.

From R7.2.1 onwards, the PBRS mode configuration is supported on the ODU2e controller on OTN-XP card.

controller Odu2e *R/S/I/P/C/L* **opu prbs mode** { **source** | **sink** | **source-sink** } **pattern invertedpn31**

Syntax Description

R/S/I/P/C/L	Rack/Slot/Instance/Port/Client-port/Lane-number of the ODU2e controller.
opu	Configures Optical Channel Payload Unit (OPU) on the ODU2e controller.
prbs mode {**source** | **sink** | **source-sink**}	Configures Pseudo Random Binary Sequence (PRBS) mode as source, sink, or source sink.
patterninvertedpn31	Configures PRBS pattern as inverted pattern. Sequence length is from 2^31 -1 bits.

Command Default None

Command Modes Configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Example

The following is a sample in which PRBS mode is configured as source with pattern as invertedpn31.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller odu2e 0/0/0/0/4/1
RP/0/RP0/CPU0:ios(config-odu2e)#opu
RP/0/RP0/CPU0:ios(config-Opuk)#prbs mode source pattern invertedpn31
RP/0/RP0/CPU0:ios(config-Opuk)#commit
```

controller ODU4

To configure the ODU4 controller, use the **controller ODU4** command in the configuration mode.

controller ODU4 *R/S/I/P* **gcc2**

Syntax Description

R/S/I/P/L	Rack/Slot/Instance/Port/Lane of the ODU4 controller.
gcc2	Enables the GCC2 interface.

Command Default None

Command Modes Configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.
Release 7.1.1	**gcc2** keyword was added.

Example

The following is a sample in which OTNSec is configured on ODU4 controllers.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 12 12:10:21.374 UTC
RP/0/RP0/CPU0:ios(config)#controller ODU4 0/1/0/0/1
RP/0/RP0/CPU0:ios(config-odu4)#otnsec
RP/0/RP0/CPU0:ios(config-otnsec)#source ipv4 10.0.0.1
RP/0/RP0/CPU0:ios(config-otnsec)#destination ipv4 10.0.0.2
RP/0/RP0/CPU0:ios(config-otnsec)#session-id 9000
RP/0/RP0/CPU0:ios(config-otnsec)#policy otnsec-policy1
RP/0/RP0/CPU0:ios(config-otnsec)#ikev2 profile1
RP/0/RP0/CPU0:ios(config-otnsec)#commit
Mon Mar 12 12:14:17.609 UTC
RP/0/RP0/CPU0:ios(config-otnsec)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

The following is a running configuration on an ODU4 controller.

```
RP/0/RP0/CPU0:ios#show run controller ODU4 0/1/0/0/1
Tue Mar 12 12:20:49.153 UTC
controller ODU40/1/0/0/1
 gcc2
 otnsec
  policy otnsec-policy1
  source ipv4 10.0.0.1
  destination ipv4 10.0.0.2
  session-id 9000
 !
!
```

The following is a sample to enable the GCC2 interface.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller odu4 0/1/0/0/1
RP/0/RP0/CPU0:ios(config-odu4)#gcc2
RP/0/RP0/CPU0:ios(config-odu4)#commit
RP/0/RP0/CPU0:ios(config-odu4)#exit
```

controller ODUC4

To configure the ODUC4 controller, use the **controller ODUC4** command in the configuration mode.

controller ODUC4 *R/S/I/P*

Syntax Description

R/S/I/P/L	Rack/Slot/Instance/Port/Lane of the ODUC4 controller.

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.8.1	This command is introduced.

Example

The following is a sample in which OTNSec is configured on ODUC4 controllers.

```
RP/0/RP0/CPU0:ios#configure
Wed Sep 28 23:10:48.429 UTC
RP/0/RP0/CPU0:ios(config)#controller oduc4 0/0/0/12
RP/0/RP0/CPU0:ios(config-oduc4)#otnsec
RP/0/RP0/CPU0:ios(config-otnsec)#source ipv4 10.1.1.1
RP/0/RP0/CPU0:ios(config-otnsec)#destination ipv4 10.1.1.2
RP/0/RP0/CPU0:ios(config-otnsec)#session-id 99
RP/0/RP0/CPU0:ios(config-otnsec)#policy otnsec-policy1
RP/0/RP0/CPU0:ios(config-otnsec)#ikev2 profile1
RP/0/RP0/CPU0:ios(config-otnsec)#commit
Wed Sep 28 23:10:48.973 UTC
RP/0/RP0/CPU0:ios(config-otnsec)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

The following is a running configuration on an ODUC4 controller.

```
RP/0/RP0/CPU0:ios#show run controller ODUC4 0/0/0/12
Wed Sep 28 23:11:418.123 UTC
controller ODUC4 0/0/0/12
 gcc2
 otnsec
  policy otnsec-policy1
  source ipv4 10.0.0.1
  destination ipv4 10.0.0.2
  session-id 99
 !
!
```

The following is a sample to enable the GCC2 interface.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller ODUC4 0/0/0/12
RP/0/RP0/CPU0:ios(config-odu4)#gcc2
RP/0/RP0/CPU0:ios(config-odu4)#commit
RP/0/RP0/CPU0:ios(config-odu4)#exit
```

controller odu-group-mp

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

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

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

Syntax Description

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

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

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

ODU group is always created on the head node.

Task ID

Task ID	Operation
otn	write

Example

This example shows how to create an ODU group controller:

```
RP/0/RP0:hostname(config)# controller odu-group-mp 2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp4)# protecting-controller ODUC4 0/0/0/13
RP/0/RP0:hostname(config-odu-group-mp4)# working-controller ODUC4 0/0/0/12
```

controller OTU (OTN-XP Card)

To configure the OTU controller, use the **controller OTU** command in the configuration mode.

From R7.2.1 onwards, you can configure loopback on the OTU2, OTU2e, and OTU4 controllers on OTN-XP card.

controller { **otu2** | **otu2e** | **otu4** } *R/S/I/P/L* **sec-admin-state loopback** [**internal** | **line**]

Syntax Description

R/S/I/P/L	Rack/Slot/Instance/Port/Lanenumber of the OTU2, OTU2e, and OTU4 controller. The range of *Lanenumber* is from 1 to 4.
sec-admin-state	Configures the administrative state of the controller .
loopback [internal | line]	Configures the internal or line loopback mode on the OTU2, OTU2e, and OTU4 controller.

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Examples

The following is a sample in which the line loopback is configured on the OTU2e controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller otu2e 0/0/0/11/3
RP/0/RP0/CPU0:ios(config-otu2e)#secondary-admin-state maintenance
RP/0/RP0/CPU0:ios(config-otu2e)#loopback line
RP/0/RP0/CPU0:ios(config-otu2e)#commit
Thu Apr 23 10:55:19.319 UTC
RP/0/RP0/CPU0:ios(config-otu2e)#end
```

The following is a sample in which the internal loopback is configured on the OTU2 controller.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller otu2 0/0/0/5/1
RP/0/RP0/CPU0:ios(config-otu2)#secondary-admin-state maintenance
RP/0/RP0/CPU0:ios(config-otu2)#loopback internal
RP/0/RP0/CPU0:ios(config-otu2)#commit
Thu Apr 23 11:01:00.562 UTC
RP/0/RP0/CPU0:ios(config-otu2)#end
```

The following is a sample in which the internal loopback is configured on the OTU4 controller.

```
RP/0/RP0/CPU0:ios#configure
```

```
RP/0/RP0/CPU0:ios(config)#controller otu4 0/0/0/0
RP/0/RP0/CPU0:ios(config-otu4)#secondary-admin-state maintenance
RP/0/RP0/CPU0:ios(config-otu4)#loopback internal
RP/0/RP0/CPU0:ios(config-otu4)#commit
Thu Apr 23 11:05:22.429 UTC
RP/0/RP0/CPU0:ios(config-otu4)#end
```

controller optics

To configure the optics controller, use the **controller optics** command in the optics controller configuration mode.

controller optics *R/S/I/P* [**baud-rate** *rate*] [**bits-per-symbol** *value*] [**cd-max** *cd-max* | **cd-min** *cd-min* | **cd-low-threshold** *cd-low* | **cd-high-threshold** *cd-high* | **dgd-high-threshold** *dgd-value* | **lbc-high-threshold** *lbc-value* | **osnr-low-threshold** *osnr-value* **description** *description* | **rx-high-threshold** *rx-high* | **rx-low-threshold** *rx-low* | **tx-high-threshold** *tx-high* | **tx-low-threshold** *tx-low* | **sec-admin-state {maintenance | normal}** | **shutdown** | **transmit-power** *transmit-power* | **transmit-shutdown** | **perf-mon** { **enable** | **disable** } | **pm** { **30-sec |15-min | 24-hour** } | **optics** { **report** | **threshold** { **cd** | **dgd** | **lbc** | **lbc-pc** | **opr** | **opr-dbm** | **opt** | **opt-dbm** | **osnr** | **pcr** | **pdl** | **pn** | **sopmd** | **rx-sig-pow** | **rx-sig-pow-dbm** } }] [**fastpoll** { **enable** | **disable** }]

To configure the sub-sea parameters for the optics controller, use the following command:

controller optics *R/S/I/P* [**filter-roll-off-factor** *value* | **filter-roll-off-factor** *value* | **rx-voa target-power** *value* | **rx-voa fixed-ratio** *value* | **enh-colorless-mode** *value* | **enh-sop-tol-mode** *value* | **nleq-comp-mode** *value* | **cross-pol-gain-mode** *value* | **cross-pol-weight-mode** *value* | **cpr-win-mode** *value* | **cpr-ext-win-mode** *value* | **submarine-params** *type value*]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port of the optics controller.
baud-rate *rate*	Sets baud-rate for this controller in GBd.
bits-per-symbol *value*	Sets bits-per-symbol for this controller.
cd-max *cd-max*	(Only for trunk optics controllers) Maximum chromatic dispersion. The range is –350000 to +350000 ps/nm.
cd-min *cd-min*	(Only for trunk optics controllers) Minimum chromatic dispersion. The range is –350000 to +350000 ps/nm.
cd-low-threshold *cd-low*	(Only for trunk optics controllers) Minimum acceptable chromatic dispersion. The CD alarm is raised if the chromatic dispersion goes below this value. The range is –350000 to +350000 ps/nm.
cd-high-threshold *cd-high*	(Only for trunk optics controllers) Maximum acceptable chromatic dispersion. The CD alarm is raised if the chromatic dispersion exceeds this value. The range is –350000 to +350000 ps/nm.

dgd-high-threshold *dgd-value*	(Only for trunk optics controllers) Configures the maximum acceptable Differential Group Delay (DGD) value. The DGD alarm is raised if DGD exceeds this value. The range is 0–18000 (in the units of 0.01 ps).
lbc-high-threshold *lbc-value*	Configures the high laser bias current threshold. The range is 0 to 100%.
osnr-low-threshold *osnr-value*	(Only for trunk optics controllers) Configures the minimum acceptable Optical Signal to Noise ratio (OSNR) value. The OSNR alarm is raised if OSNR goes below this value. The range is 0–4000 (in units of 0.01db).
description *description*	Description of the optics controller.
rx-high-threshold *rx-high*	Configures high receive power threshold. The range is –400 to 300 (in the units of 0.1 dBm).
rx-low-threshold *rx-low*	Configures low receive power threshold. The range is –400 to 300 (in the units of 0.1 dBm).
tx-high-threshold *tx-high*	Configures high transmit power threshold. The range is –400 to 300 dBm (in the units of 0.1 dBm).
tx-low-threshold *tx-low*	Configures low transmit power threshold. The range is –400 to 300 dBm (in the units of 0.1 dBm).
sec-admin-state	Configures the administrative state of the controller. The values are maintenance or normal.
shutdown	Disables the configuration of the controller.
pm	Configures performance monitoring parameters for 30 second, 15 minute, and 24-hour intervals.
transmit-power *transmit-power*	(Only for trunk optics controllers) Configures the transmit power. The range is –190 to 30 dBm (in the units of 0.1 dBm). From Release 7.3.1 onwards, transmit power is supported on the CFP2 DCO optics for the OTN-XP card. The transmit power value is –10 to +1 dBm.
transmit-shutdown	Shuts down the transmit laser.
perf-mon { **enable** | **disable** }	Enables or disables performance monitoring.
cd	Configures the chromatic dispersion threshold.
dgd	Configures the differential group delay threshold.
lbc	Configures the laser bias current threshold.

lbc-pc	Configures the laser bias current threshold in percentage.
opr	Configures the optical Rx power threshold in uW.
opr-dbm	Configures the optical Rx power threshold in dBm. The unit is 0.01 dBm. For example, if you want to configure 30.00 dBm, enter 3000.
opt	Configures the optical Tx power threshold in uW.
opt-dbm	Configures the optical Tx power threshold in dBm. The unit is 0.01 dBm.
osnr	Configures the OSNR threshold.
pcr	Configures the Polarization Change Rate (PCR) threshold.
pdl	Configures the Polarization-Dependent Loss (PDL) threshold.
pn	Configures the Phase Noise (PN) threshold.
sopmd	Configures the Second Order Polarization Mode Dispersion (SOPMD) threshold.
rx-sig-pow	Configures the Rx signal power threshold in uW.
rx-sig-pow-dbm	Configures the Rx signal power threshold in dBm. The unit is 0.01 dBm.
filter-roll-off-factor *value*	Configures the RRC filter roll-off factor. The range is 0 to 1.
rx-voa target-power *value*	Configures the receive target power. The range is –190 to +30.
rx-voa fixed-ratio *value*	Configures the receive ratio of optical attenuation. The range is +100 to +1700.
enh-colorless-mode *value*	Configures the enhanced colorless mode. The range is 1–3.
enh-sop-tol-mode *value*	Configures the enhanced SOP tolerance mode. The range is 1–3.
nleq-comp-mode *value*	Configures the non-linear compensation. The range is 1–4.
cross-pol-gain-mode *value*	Configures the carrier phase recovery cross polarization gain mode. The range is 0–15.
cross-pol-weight-mode *value*	Configures the carrier phase recovery cross polarization weight mode. The range is 0–15.
cpr-win-mode *value*	Configures the carrier phase recovery window mode. The range is 1–4.
cpr-ext-win-mode *value*	Configures the carrier phase recovery extended window mode. The range is 1–9.
submarine-params *type value*	Configures the proprietary submarine parameters. The range for the type is 1–10 and the range for the value is 1–1000. **Note** This parameter is for future use.

fastpoll { **enable** | **disable** }	Enables or disables fast polling of SOP data.

Command Default

None

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.3.1	The keyword **fastpoll** was added.

Command Modes

Optics controller configuration

Usage Guidelines

The configurations for chromatic dispersion (cd-max, cd-min, cd-low-threshold, and cd-high-threshold) must be performed only after the **hw-module** configuration. These configurations must be removed before the **no hw-module** configuration.

Example

The following example shows how to configure the optics controller and set the high-power threshold at the transmit and receive side.

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)#controller optics 0/0/1/1
RP/0/RP0/CPU0:ios(config-optics)#rx-high-threshold 200
RP/0/RP0/CPU0:ios(config-optics)#tx-high-threshold 300
```

The following example shows how to configure the optics controller and set the ranges for chromatic dispersion.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller optics 0/0/1/1
RP/0/RP0/CPU0:ios(config-optics)#cd-max 10000
RP/0/RP0/CPU0:ios(config-optics)#cd-min 2000
```

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

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller optics 0/0/1/1 pm 24-hour optics threshold osnr max
345
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the fastpoll data is enabled on the optics controller:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)# [no] controller optics <r/s/i/p> fastpoll enable
```

The following is a sample to configure transmit power on the CFP2 DCO optics for the OTN-XP card:

```
RP/0/RP0/CPU0:ios#configure
Mon Aug 19 19:31:42.115 UTC
RP/0/RP0/CPU0:ios(config)#controller optics 0/1/0/12
```

```
RP/0/RP0/CPU0:ios(config-Optics)#transmit-power -1.50
RP/0/RP0/CPU0:ios(config-Optics)#commit
Mon Aug 19 19:35:24.697 UTC
RP/0/RP0/CPU0:ios(config-Optics)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

The following is a sample to configure 8QAM modulation on the 200G muxponder mode for the OTN-XP card:

```
RP/0/RP0/CPU0:ios#configure
Wed Jun 2 17:21:42.115 UTC
RP/0/RP0/CPU0:ios(config)#controller optics 0/1/0/12
RP/0/RP0/CPU0:ios(config-Optics)#bits-per-symbol 3
RP/0/RP0/CPU0:ios(config-Optics)#commit
```

crypto ca authenticate

To authenticate the certification authority (CA) by getting the certificate for the CA, use the **crypto ca authenticate** command in EXEC mode.

crypto ca authenticate { *ca-name* | **system-trustpoint** }

Syntax Description

ca-name	Name of the CA Server.
system-trustpoint	Generates self-signed root certificate.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

The **crypto ca authenticate** command is required when you initially configure CA support at your NCS 1004.

This command authenticates the CA to your NCS 1004 by obtaining the CA certificate, which contains the public key for the CA. For self-signed root CA, because the CA signs its own certificate, you should manually authenticate the CA public key by contacting the CA administrator when you use this command. The certificate fingerprint matching is done out-of-band (for example, phone call, and so forth).

Authenticating a second-level CA requires prior authentication of the root CA.

After the **crypto ca authenticate** command is issued and the CA does not respond by the specified timeout period, you must obtain terminal control again to re-enter the command.

Task ID

Task ID	Operations
crypto	execute

Examples

The CA sends the certificate, and the NCS 1004 prompts the administrator to verify the certificate by checking the certificate fingerprint (a unique identifier). The CA administrator can also display the CA certificate fingerprint, so you should compare what the CA administrator sees to what the NCS 1004 displays on the screen. If the fingerprint on the display matches the fingerprint displayed by the CA administrator, you should accept the certificate as valid.

The following example shows that the NCS 1004 requests the CA certificate:

```
RP/0/0RP0RSP0/CPU0:ios# crypto ca authenticate msiox
Retrieve Certificate from SFTP server? [yes/no]: yes
Read 860 bytes as CA certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Certificate has the following attributes:
   Fingerprint: D0 44 36 48 CE 08 9D 29 04 C4 2D 69 80 55 53 A3

Do you accept this certificate? [yes/no]: yes


RP/0/0RP0RSP0/CPU0:ios: cepki[335]: %SECURITY-CEPKI-6-INFO : certificate database updated
Do you accept this certificate? [yes/no] yes
```

This example shows how to generate a self-signed root certificate:

```
RP/0/0RP0RSP0/CPU0:ios#crypto ca authenticate system-trustpoint
```

crypto ca enroll

To obtain a NCS 1004 certificate from the certification authority (CA), use the **crypto ca enroll** command in EXEC mode.

crypto ca enroll { *ca-name* | **system-trustpoint** }

Syntax Description

ca-name	Name of the CA Server.
system-trustpoint	Generates the leaf certificate.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **crypto ca enroll** command to request certificates from the CA for the Rivest, Shamir, and Adelman (RSA) key pairs for NCS 1004 defined by the rsakeypair, on page 105 command in trustpoint configuration mode. If no **rsakeypair** command is configured for the current trustpoint, the default RSA key pair is used for enrollment. This task is also known as enrolling with the CA. (Enrolling and obtaining certificates are two separate events, but they both occur when the **crypto ca enroll** command is issued.) When using manual enrollment, these two operations occur separately.

NCS 1004 needs a signed certificate from the CA for each of the RSA key pairs on NCS 1004; if you previously generated general-purpose keys, this command obtains the one certificate corresponding to the one general-purpose RSA key pair. If you previously generated special-usage keys, this command obtains two certificates corresponding to each of the special-usage RSA key pairs.

If you already have a certificate for your keys, you are unable to configure this command; instead, you are prompted to remove the existing certificate first. (You can remove existing certificates by removing the trustpoint configuration with the **no crypto ca trustpoint** command.)

The **crypto ca enroll** command is not saved in NCS 1004 configuration.

Note The root certificate signs the leaf certificate.

Task ID

Task ID	Operations
crypto	execute

Examples

The following sample output is from the **crypto ca enroll** command:

```
RP/0/0RP0RSP0/CPU0:ios# crypto ca enroll msiox
% Start certificate enrollment...
% Create a challenge password. You will need to verbally provide this password to the
  CA Administrator in order to revoke your certificate.
% For security reasons you password will not be saved in the configuration.
% Please make a note of it.
%Password
re-enter Password:
    Fingerprint: 4F35ADC9 2791997A CE211437 AFC66CF7

RP/0/0RP0RSP0/CPU0:May 29 18:49:15.572 : pki_cmd: %PKI-6-LOG_INFO : certificate request
pending

RP/0/0RP0RSP0/CPU0:May 29 18:52:17.705 : pki_get_cert: %PKI-6-LOG_INFO : certificate is
granted
```

This example shows how to generate a leaf certificate:

```
RP/0/0RP0RSP0/CPU0:ios#crypto ca enroll system-trustpoint
```

crypto ca trustpoint

To configure a trusted point with a selected name, use the **crypto ca trustpoint** command. To unconfigure a trusted point, use the **no** form of this command in Config mode.

crypto ca trustpoint { *ca-name* | **system-trustpoint** }

Syntax Description

ca-name	Name of the CA.
system-trustpoint	Specifies the default system trustpoint.

Command Default

None

Command Modes

Config mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA.

This command allows you to configure a trusted point with a selected name so that NCS 1004 can verify certificates issued to peers. NCS 1004 need not enroll with the CA that issued the certificates to the peers.

The **crypto ca trustpoint** command enters trustpoint configuration mode, in which you can specify characteristics for the CA with a set of commands. See the Related Commands section for details.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to use the **crypto ca trustpoint** command to create a trustpoint:

```
RP/0/0RP0RSP0/CPU0:ios# configure
RP/0/0RP0RSP0/CPU0:ios(config)# crypto ca trustpoint msiox
RP/0/0RP0RSP0/CPU0:ios(config-trustp)# sftp-password xxxxxx
RP/0/0RP0RSP0/CPU0:ios(config-trustp)# sftp-username tmordeko
RP/0/0RP0RSP0/CPU0:ios(config-trustp)# enrollment url
sftp://192.168..254.254/tftpboot/tmordeko/CAcert
RP/0/0RP0RSP0/CPU0:ios(config-trustp)# rsakeypair label-2
```

This example shows how to create a default system trustpoint:

```
RP/0/0RP0RSP0/CPU0:ios#configure
RP/0/0RP0RSP0/CPU0:ios(config)#crypto ca trustpoint system-trustpoint
RP/0/0RP0RSP0/CPU0:ios(config-trustp)#commit
```

Command	Description
enrollment retry count, on page 46	Specifies how many times NCS 1004 resends a certificate request.
enrollment retry period, on page 47	Specifies the wait period between certificate request retries.
enrollment terminal, on page 48	Specifies manual cut-and-paste certificate enrollment.
enrollment url, on page 48	Specifies the URL of the CA.
query url, on page 103	Specifies the LDAP URL of the CRL distribution point. Required only if your CA supports Lightweight Directory Access Protocol (LDAP).
rsakeypair, on page 105	Specifies a named RSA key pair for this trustpoint.
sftp-password (trustpoint), on page 105	Secures the FTP password.
sftp-username (trustpoint), on page 106	Secures the FTP username.
subject-name (trustpoint), on page 160	Specifies a subject name in the certificate request.

crypto key generate dsa

To generate Digital Signature Algorithm (DSA) key pairs, use the **crypto key generate dsa** command in EXEC mode.

crypto key generate dsa [**system-enroll-key** | **system-root-key**]

Syntax Description

system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in Config Mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in Config Mode does not support this option.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **crypto key generate dsa** command to generate DSA key pairs for your NCS 1004.

DSA keys are generated in pairs—one public DSA key and one private DSA key.

If NCS 1004 already has DSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys.

To remove the DSA key generated in Config mode, use **no** form of this command in Config mode.

To remove the DSA key generated in EXEC mode, use the **crypto key zeroize dsa** command.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to generate a 512-bit DSA key:

```
RP/0/RP0/CPU0:ios# crypto key generate dsa
The name for the keys will be: the_default
    Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits.
Choosing a key modulus
How many bits in the modulus [1024]: 512
Generating DSA keys...
Done w/ crypto generate keypair
[OK]
```

This example shows how to generate a DSA key pair for the root certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate dsa system-root-key
```

This example shows how to generate a DSA key pair for the leaf certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate dsa system-enroll-key
```

The following example shows how to generate a 512-bit DSA key-pair in Config mode:

```
RP/0/RP0/CPU0:ios#conf t
RP/0/RP0/CPU0:ios(config)#crypto key generate dsa 512
RP/0/RP0/CPU0:ios(config)#commit
```

This example shows how to delete a DSA key-pair in Config mode:

```
RP/0/RP0/CPU0:ios# conf t
RP/0/RP0/CPU0:ios(config)#no crypto key generate dsa 512
RP/0/RP0/CPU0:ios(config)#commit
```

crypto key generate ecdsa

To generate an Elliptic Curve Digital Signature Algorithm (ECDSA) key pair, use the **crypto key generate ecdsa** command in EXEC mode.

crypto key generate ecdsa [**nistp256** | **nistp384** | **nistp521**] [**system-enroll-key** | **system-root-key**]

Syntax Description

nistp256	Generates an ECDSA key of curve type nistp256, with key size 256 bits.
nistp384	Generates an ECDSA key of curve type nistp384, with key size 384 bits.
nistp521	Generates an ECDSA key of curve type nistp521, with key size 521 bits.

system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in Config Mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in Config Mode does not support this option.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

To remove the ECDSA key generated in Config mode, use **no** form of this command in Config mode.

To remove an ECDSA key generated in EXEC mode, use the **crypto key zeroize ecdsa** command.

Task ID

Task ID	Operation
crypto	execute

Examples

The following example shows how to generate an ECDSA key pair:

```
RP/0/RP0/CPU0:ios# crypto key generate ecdsa nistp384
Wed Mar 28 12:53:57.355 UTC
% You already have keys defined for the_default
Do you really want to replace them? [yes/no]: yes
Generating ECDSA keys ...
Done w/ crypto generate ECDSA keypair
[OK]
```

This example shows how to generate a ECDSA key pair for the root certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate ecdsa system-root-key
```

This example shows how to generate a ECDSA key pair for the leaf certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate dsa system-enroll-key
```

The following example shows how to generate an ECDSA key-pair in Config mode:

```
RP/0/RP0/CPU0:ios#conf t
RP/0/RP0/CPU0:ios(config)#crypto key generate ecdsa nistp256
RP/0/RP0/CPU0:ios(config)#commit
```

This example shows how to delete en ECDSA key-pair in Config mode:

```
RP/0/RP0/CPU0:ios# conf t
RP/0/RP0/CPU0:ios(config)#no crypto key generate ecdsa nistp256
RP/0/RP0/CPU0:ios(config)#commit
```

crypto key generate ed25519

To generate Ed25519 crypto key pairs as part of supporting the Ed25519 public-key signature system, use the **crypto key generate ed25519** command in EXEC mode and Config mode.

crypto key generate ed25519 [**system-enroll-key** | **system-root-key**]

Syntax Description

system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in Config mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in Config mode does not support this option.

Command Default

None

Command Modes

EXEC mode and Config mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit platforms.

To remove the Ed25519 key generated in Config mode, use **no** form of this command in Config mode.

To remove the Ed25519 key generated in EXEC mode, use the **crypto key zeroize ed25519** command.

You can generate the crypto keys either with an empty label or with two predefined labels (**system-root-key** and **system-enroll-key**). In case of empty label, the system generates the key pair against the default label. The key pairs with the predefined labels are used to integrate Cisco IOS XR with Cisco Crosswork Trust Insights.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to generate a Ed25519 crypto key pair:

```
RP/0/RP0/CPU0:ios# crypto key generate ed25519

Mon Nov 30 07:03:17.058 UTC
The name for the keys will be: the_default
Generating ED25519 keys ...
Done w/ crypto generate keypair
```

```
[OK]
```

This example shows how to generate a Ed25519 crypto key pair for the root certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate ed25519 system-root-key
```

This example shows how to generate a Ed25519 crypto key pair for the leaf certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate ed25519 system-enroll-key
```

The following example shows how to generate an Ed25519 key-pair in Config mode:

```
RP/0/RP0/CPU0:ios#conf t
RP/0/RP0/CPU0:ios(config)#crypto key generate ed25519
RP/0/RP0/CPU0:ios(config)#commit
```

This example shows how to delete en Ed25519 key-pair in Config mode:

```
RP/0/RP0/CPU0:ios# conf t
RP/0/RP0/CPU0:ios(config)#no crypto key generate ed25519
RP/0/RP0/CPU0:ios(config)#commit
```

Related Commands

Command	Description
crypto key zeroize ed25519, on page 39	Deletes Ed25519 crypto key pairs from NCS 1004.
show crypto key mypubkey ed25519, on page 114	Displays the Ed25519 public keys of NCS 1004.

crypto key generate rsa

To generate a Rivest, Shamir, and Adelman (RSA) key pair, use the **crypto key generate rsa** command in EXEC mode and Config mode.

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

Syntax Description

usage-keys	(Optional) Generates separate RSA key pairs for signing and encryption.
general-keys	(Optional) Generates a general-purpose RSA key pair for signing and encryption.
keypair-label	(Optional) RSA key pair label that names the RSA key pairs.
system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in Config mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in Config mode does not support this option.

Command Default

RSA key pairs do not exist.

If the **usage-keys** keyword is not used, general-purpose keys are generated. If no RSA label is specified, the key is generated as the default RSA key.

Command Modes

EXEC mode and Config mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **crypto key generate rsa** command to generate RSA key pairs for NCS 1004.

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If NCS 1004 already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys. The keys generated by this command are saved in the secure NVRAM (which is not displayed to the user or backed up to another device).

To remove an RSA key generated in Config mode, use **no** form of this command in Config mode.

To remove an RSA key generated in EXEC mode, use the **crypto key zeroize rsa** command.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to generate an RSA key pair:

```
RP/0/RP0/CPU0:ios# crypto key generate rsa

The name for the keys will be: the_default

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus[1024]: <return>
RP/0/RP0/CPU0:ios#
```

This example shows how to generate an RSA key pair for the root certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate rsa system-root-key
```

This example shows how to generate an RSA key pair for the leaf certificate:

```
RP/0/RP0/CPU0:ios#crypto key generate rsa system-enroll-key
```

The following example shows how to generate an RSA key-pair in Config mode:

```
RP/0/RP0/CPU0:ios#conf t
RP/0/RP0/CPU0:ios(config)#crypto key generate rsa user1 general-keys 2048
RP/0/RP0/CPU0:ios(config)#commit
```

This example shows how to delete en RSA key-pair in Config mode:

```
RP/0/RP0/CPU0:ios# conf t
RP/0/RP0/CPU0:ios(config)#no crypto key generate rsa user1 general-keys 2048
RP/0/RP0/CPU0:ios(config)#commit
```

crypto key import authentication rsa

To import a public key using the Rivest, Shamir, and Adelman (RSA) method, use the **crypto key import authentication rsa** command in EXEC mode.

crypto key import authentication rsa *path*

Syntax Description

path	(Optional) This denotes the path to the RSA public key file.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

1. Use shh-keygen generation mechanism to generate keys using either a LINUX or UNIX client. This creates two keys: one public and one private.
2. Remove the comment and other header tag from the keys, except the base64encoded text.
3. Decode the base64encoded text, and use the for authentication.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example displays how to import a public key:

```
RP/0/RP0/CPU0:ios:hostname#crypto key import authentication rsa
```

crypto key zeroize ed25519

To delete the Ed25519 crypto key pair from NCS 1004, use the **crypto key zeroize ed25519** command in EXEC mode.

crypto key zeroize ed25519

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	execute

Examples This example shows how to delete Ed25519 crypto key pairs from NCS 1004:

```
RP/0/0RP0RSP0/CPU0:ios# crypto key zeroize ed25519
% Keys to be removed are named the_default
Do you really want to remove these keys? [yes/no]: yes
```

Related Commands

Command	Description
crypto key generate ed25519, on page 36	Generates Ed25519 crypto key pairs.
show crypto key mypubkey ed25519, on page 114	Displays the Ed25519 public keys of NCS 1004.

crypto key zeroize rsa

To delete all Rivest, Shamir, and Adelman (RSA) keys from NCS 1004, use the **crypto key zeroize rsa** command in EXEC mode.

crypto key zeroize rsa [*keypair-label*]

Syntax Description

keypair-label	(Optional) Names the RSA key pair to be removed.

Command Default If the key pair label is not specified, the default RSA key pair is removed.

Command Modes EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **crypto key zeroize rsa** command to delete all RSA keys that were previously generated by NCS 1004. After issuing this command, you must perform two additional tasks:

- Ask the certification authority (CA) administrator to revoke the certificates for NCS 1004 at the CA; you must supply the challenge password you created when you originally obtained NCS 1004 certificates with the crypto ca enroll, on page 30 command CA.
- Manually remove the certificates from the configuration using the **clear crypto ca certificates** command.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to delete the general-purpose RSA key pair that was previously generated:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# crypto key zeroize rsa key1
% Keys to be removed are named key1
Do you really want to remove these keys? [yes/no]: yes
```

destination address

To specify the destination address for Smart Call Home, use the **destination address** command in the call home profile configuration mode.

destination address *address*

Syntax Description

address	Specifies the destination address for Smart Call Home. The format is {http|https}://{FQDN}/its/service/oddce/services/DDCEService FQDN must be either Cisco Smart Software Manager FQDN (tools.cisco.com) or Smart Licensing satellite server FQDN.

Command Default

None

Command Modes

Call home profile configuration mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

You must configure the DNS server before setting-up the call-home destination address as FQDN. Use **domain name-server {DNS server IP}** command to configure the DNS server on the device.

The following example shows how to specify the destination address for Smart Call Home.

```
domain name-server 192.0.2.6
call-home
service active
contact smart-licensing
profile CiscoTAC-1
active
destination address http https://bst.cloudapps.cisco.com/bugsearch
```

destination ipv4 unicast

To specify the destination of a GMPLS UNI tunnel, use the **destination ipv4 unicast** command in GMPLS UNI controller tunnel-properties configuration sub-mode.

destination ipv4 unicast *address*

Syntax Description

address	Specifies the tunnel destination (IPv4 address).

Command Default

None

Command Modes

GMPLS UNI controller tunnel-properties configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to specify a tunnel destination (10.10.3.4).

```
RP/0/RP0/CPU0:ios(config)#mpls traffic-eng
RP/0/RP0/CPU0:ios(config-mpls-te)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-te-gmpls)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-te-gmpls-cntl)#tunnel-properties
RP/0/RP0/CPU0:ios(config-te-gmpls-tun)#destination 10.10.3.4
RP/0/RP0/CPU0:ios(config-te-gmpls-tun)#
```

destination transport-method

To specify the destination transport method for Smart Call Home, use the **destination transport-method** command.

destination transport-method {http|email}

Syntax Description

email	Enables an e-mail address for the profile.
http	Enables an HTTP URL for the profile.

Command Default None

Command Modes Call home profile configuration mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines For the user profile, both e-mail and http can be enabled. For the Cisco TAC profile, only one transport method can be enabled.

The following example shows how to specify the destination transport method for Smart Call Home.

```
domain name-server 192.0.2.6
call-home
service active
contact smart-licensing
profile CiscoTAC-1
active
destination address http https://bst.cloudapps.cisco.com/bugsearch
destination transport-method http
```

dh

To specify the Diffie-Hellman group for the IKEv2 proposal, use the **dh** command in IKEv2 proposal configuration mode.

dh *dh-group*

Syntax Description

dh-group	DH group identifier. The possible values are 19, 20, and 21.

Command Default None

Command Modes IKEv2 proposal configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 proposal is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 19:19:30.259 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 proposal proposal1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#encryption aes-cbc-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#integrity sha-1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#prf sha-256
```

```
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#dh 20
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#commit
Thu Mar  7 19:20:30.916 UTC
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 proposal proposal1
Thu Mar  7 19:20:48.929 UTC

Proposal Name              : proposal1
================================================================================
Status                     : Complete
--------------------------------------------------------------------------------
Total Number of Enc. Alg.  : 1
   Encr. Alg.              : CBC-AES-256
--------------------------------------------------------------------------------
Total Number of Hash. Alg. : 1
   Hash. Alg.              : SHA 1
--------------------------------------------------------------------------------
Total Number of PRF. Alg.  : 1
   PRF. Alg.               : SHA 256
--------------------------------------------------------------------------------
Total Number of DH Group   : 1
   DH Group                : Group 20
```

dwdm-carrier

To configure the wavelength on the trunk port, use the **dwdm-carrier** command in optics controller configuration mode. To return the wavelength to its default value, use the **no** form of this command.

dwdm-carrier { **100MHz-grid** **frequency** *frequency* } | { **50GHz-grid** **frequency** *frequency* }

Syntax Description

50Ghz-grid | **100MHz-grid**	Configures the wavelength in 50GHz grid and 100MHz (0.1GHz) grid spacing respectively in accordance with ITU definition.
frequency *frequency*	Specifies the frequency for the optics controller.

Command Default

None

Command Modes

Optics controller configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The controller must be in the shutdown state before you can use the **wavelength** command.

Example

The following example shows how to configure the frequency in 100MHz grid spacing.

```
RP/0/RP0/CPU0:ios# config
```

```
RP/0/RP0/CPU0:ios(config)# controller optics 0/0/0/0
RP0/0/CPU0:ios(config-optics)# dwdm-carrier 100MHz-grid frequency 1865000
```

encryption

To specify the transform types for encryption, use the **encryption** command in the IKEv2 proposal configuration mode.

encryption *encryption-type*

Syntax Description

encryption-type	Encrytion algorithm. The possible values are aes-gcm-256, aes-gcm-128, aes-cbc-256, aes-cbc-192, and aes-cbc-128.

Command Default

None

Command Modes

IKEv2 proposal configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 proposal is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 19:19:30.259 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 proposal proposal1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#encryption aes-cbc-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#integrity sha-1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#prf sha-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#dh 20
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#commit
Thu Mar  7 19:20:30.916 UTC
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 proposal proposal1
Thu Mar  7 19:20:48.929 UTC

Proposal Name              : proposal1
================================================================================
Status                     : Complete
--------------------------------------------------------------------------------

Total Number of Enc. Alg.  : 1
   Encr. Alg.              : CBC-AES-256

--------------------------------------------------------------------------------
Total Number of Hash. Alg. : 1
   Hash. Alg.              : SHA 1
--------------------------------------------------------------------------------
Total Number of PRF. Alg.  : 1
   PRF. Alg.               : SHA 256
```

```
--------------------------------------------------------------------------------
Total Number of DH Group   : 1
   DH Group                : Group 20
```

enrollment retry count

To specify the number of times a NCS 1004 resends a certificate request to a certification authority (CA), use the **enrollment retry count** command in trustpoint configuration mode. To reset the retry count to the default, use the **no** form of this command.

enrollment retry count *number*
no enrollment retry count *number*

Syntax Description

number	Number of times NCS 1004 resends a certificate request when NCS 1004 does not receive a certificate from the previous request. The range is from 1 to 100.

Command Default

If no retry count is specified, the default value is 10.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

After requesting a certificate, NCS 1004 waits to receive a certificate from the CA. If NCS 1004 does not receive a certificate within a specified time (the retry period), NCS 1004 sends another certificate request. NCS 1004 continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

To reset the retry count to the default of 10, use the **no** form of this command. Setting the retry count to 0 indicates an infinite number of retries. NCS 1004 sends the CA certificate requests until a valid certificate is received (there is no limit to the number of retries).

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to declare a CA, change the retry period to 10 minutes, and change the retry count to 60 retries. NCS 1004 resends the certificate request every 10 minutes until receipt of the certificate or approximately 10 hours pass since the original request was sent, whichever occurs first (10 minutes x 60 tries = 600 minutes = 10 hours).

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)# crypto ca trustpoint myca
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# enrollment url http://ca_server
```

```
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# enrollment retry period 10
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# enrollment retry count 60
```

enrollment retry period

To specify the wait period between certificate request retries, use the **enrollment retry period** command in trustpoint configuration mode. To reset the retry period to the default of 1 minute, use the **no** form of this command.

enrollment retry period *minutes*
no enrollment retry period *minutes*

Syntax Description

minutes	Period (in minutes) between certificate requests issued to a certification authority (CA) from NCS 1004. The range is from 1 to 60 minutes.

Command Default

minutes: *1*

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

After requesting a certificate, NCS 1004 waits to receive a certificate from the CA. If NCS 1004 does not receive a certificate within a specified time (the retry period), NCS 1004 sends another certificate request. NCS 1004 continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

NCS 1004 sends the CA another certificate request every minute until a valid certificate is received. (By default, NCS 1004 sends ten requests, but you can change the number of permitted retries with the **enrollment retry count** command.)

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to declare a CA and change the retry period to 5 minutes:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)# crypto ca trustpoint myca
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# enrollment retry period 5
```

enrollment terminal

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal
no enrollment terminal

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

You can manually cut and paste certificate requests and certificates when you do not have a network connection between NCS 1004 and certification authority (CA). When the **enrollment terminal** command is enabled, NCS 1004 displays the certificate request on the console terminal, which allows you to enter the issued certificate on the terminal.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually specify certificate enrollment through cut-and-paste. In this example, the CA trustpoint is myca.

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)# crypto ca trustpoint myca
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# enrollment terminal
```

enrollment url

To specify the certification authority (CA) location by naming the CA URL, use the **enrollment url** command in trustpoint configuration mode. To remove the CA URL from the configuration, use the **no** form of this command.

enrollment url *CA-URL*
no enrollment url *CA-URL*

Syntax Description

CA-URL	URL of the CA server. The URL string must start with http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA (for example, http://ca-server). If the CA cgi-bin script location is not /cgi-bin/pkiclient.exe at the CA (the default CA cgi-bin script location), you must also include the nonstandard script location in the URL, in the form of http://CA-name/script-location, where script-location is the full path to the CA scripts.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **enrollment url** command to specify the CA URL. This command is required when you declare a CA with the **crypto ca trustpoint** command. The URL must include the CA script location if the CA scripts are not loaded into the default cgi-bin script location. The CA administrator should be able to tell you where the CA scripts are located.

This table lists the available enrollment methods.

Table 1: Certificate Enrollment Methods

Enrollment Method	Description
SFTP	Enroll through SFTP: file system
TFTP[1]	Enroll through TFTP: file system

[1] If you are using TFTP for enrollment, the URL must be in the form tftp://certserver/file_specification. (The file specification is optional.)

TFTP enrollment sends the enrollment request and retrieves the certificate of the CA and the certificate of NCS 1004. If the file specification is included in the URL, NCS 1004 appends an extension to the file specification.

To change the CA URL, repeat the **enrollment url** command to overwrite the previous URL

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the absolute minimum configuration required to declare a CA:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)#crypto ca trustpoint myca
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)#enrollment url
http://ca.domain.com/certsrv/mscep/mscep.dll
```

fault-profile

Use the **fault-profile** command in the global configuration mode, to create a new fault profile with one or more alarms and user-defined severity.

fault-profile *name* **fault-identifier subsystem XR fault-type** { **ethernet** | **sdh_controller** | **sonet** | **OPTICS** | **G709** } **fault-tag** *name* **sas** *severity* **nsas** *severity*

Syntax Description

fault-profile *name*	Name of the fault profile.
fault-identifier subsystem XR	Supports the XR sub-system.
fault-type	The component the fault profile is applicable to. The available options are: • ethernet • sdh_controller • sonet • OPTICS • G709
fault-tag *name*	The faults that are included as part of the newly created fault profile.
sas *severity* **nsas** *severity*	Sets the severity level for: • sas (service affecting; impacts traffic) • nsas (non-service affecting; does not impact traffic) The available options are: • Critical • Major • Minor • Non-faulted • Non-reported

Command Default

No default behavior or values.

Command Modes

Global Configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.
Release 7.2.1	

Example

The following example shows how to use the **fault profile** command.

```
RP/0/RP0/CPU0: router (config) # fault profile f1 fault-identifier subsystem XR fault-type
 HW_OPTICS fault-tag OPTICAL_LO_RXPOWER sas CRITICAL nsas CRITICAL
```

fault-profile apply

Use the **fault-profile apply** command in the global configuration mode, to apply a fault profile at the node level or card levelport level or node level.

fault-profile *name* **apply rack0 slot** *location*

Syntax Description

fault-profile *name*	Name of the fault profile.
rack 0 slot *location*	Sets the profile at the node level or line card levelport level or node level.

Command Default

No default behavior or values.

Command Modes

Global Configuration

Command History

Release	Modification
Release 7.1.1	This command was introduced.
Release 7.2.1	

Example

The following example shows how to use the **fault profile apply** command.

```
RP/0/RP0/CPU0:ios(config)# fault profile f1 apply rack 0 slot ALL
```

The following example shows how to use the **fault profile apply** command at the port level.

```
RP/0/RP0/CPU0:ios(config)# fault profile f1 apply rack 0 slot LC0 port 1
```

The following example shows how to use the **fault profile apply** command at the node level.

```
RP/0/RP0/CPU0:ios(config)# fault profile f1 apply rack 0 slot ALL
```

gmpls optical-uni

To enable GMPLS UNI feature, use the **gmpls optical-uni** command in LMP configuration mode.

gmpls optical-uni

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

LMP configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines

The LMP submode enables GMPLS-UNI LMP functionality and acts as a container for other GMPLS-UNI LMP configuration commands.

Example

The following example shows how to enable GMPLS UNI and enter LMP configuration mode.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls)#
```

http client connection

To configure the connection for http client, use the **http client connection** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client connection { **retry** *count* | **timeout** *seconds* }

Syntax Description

retry *count*	Specifies how many times HTTP Client resends a connection request. Range is from 1 to 5. The default value is 0.
timeout *seconds*	The time interval (in seconds) that HTTP client waits for a server connection to establish before giving up. Range is from 1 to 60 seconds. The default value is 10 seconds.

Command Default

The connection retry is not configured by default. The default connection timeout is set to 10 seconds.

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Command Modes

HTTP configuration

Usage Guidelines

Use this command to set the connection timeout or connection retry count.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the connection request retry to two times:

```
RP/0/RP0/CPU0:router(config)#http client connection retry 2
```

The following example shows how to configure the connection request timeout to 20 seconds:

```
RP/0/RP0/CPU0:router(config)#http client connection timeout 20
```

http client response

To configure the time interval (in seconds) for HTTP Client to wait for a response from the server before giving up, use the **http client response** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client response { **timeout** *seconds* }

Syntax Description

timeout *seconds*	The time interval (in seconds) that HTTP client waits for a response from the server before giving up. Range is from 1 to 300 seconds. The default value is 30 seconds.

Command Default

The response timeout is 30 seconds by default.

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Command Modes

HTTP configuration

Usage Guidelines

Use this command to configure the response timeout.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the response timeout to 40 seconds:

```
RP/0/RP0/CPU0:router(config)#http client response timeout 40
```

http client ssl

To configure Secure Socket Layer (SSL) version to be used for HTTPS requests, use the **http client ssl** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client ssl *version*

Syntax Description

ssl *version*	Specify the SSL version to be used for HTTPS requests. Select one of the following versions: • **tls1.0** - Forces TLSv1.0 to be used for HTTPS requests. • **tls1.1** - Forces TLSv1.1 to be used for HTTPS requests. • **tls1.2** - Forces TLSv1.2 to be used for HTTPS requests. By default libcurl does not force the TLS version.

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Command Default

By default, the SSL version is not configured.

Command Modes

HTTP configuration

Usage Guidelines

Use this command to configure the ssl version to be used in HTTPS requests.

Task ID

Task ID	Operations
config-servicess	read, write

The following example shows how to configure the SSL version to tls1.1:

```
RP/0/RP0/CPU0:router(config)#http client ssl tls1.1
```

http client secure-verify-host

To enable verifying host in peer's certificate, use the **http client secure-verify-host** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client secure-verify-host

Syntax Description

secure-verify-host	Verifies the host in peer's certificate. This is enabled by default. To disable, use the command **http client secure-verify-host** *disable*

Command Default

Host verification is enabled by default.

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Command Modes

HTTP configuration

Usage Guidelines

Use the **http client secure-verify-host** command to disable the host verification.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to disable host verification :

```
RP/0/RP0/CPU0:router(config)#http client secure-verify-host disable
```

http client secure-verify-peer

To enable verifying authenticity of the peer certificate, use the **http client secure-verify-peer** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client secure-verify-peer

Syntax Description

secure-verify-peer	Verifies authenticity of the peer certificate. This is enabled by default. To disable, use the command **http client secure-verify-peer** *disable*

Command Default

Peer verification is enabled by default.

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Command Modes

HTTP configuration

Usage Guidelines

Use the **http client secure-verify-peer** command to disable the peer verification.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to disable peer verification :

```
RP/0/RP0/CPU0:router(config)#http client secure-verify-peer disable
```

http client source interface

To specify the interface for source address for Hypertext Transfer Protocol (HTTP) connections, use the **http client source-interface** command in XR Config mode. To remove the **http client source-interface**command from the configuration file and restore the system to its default condition, use the **no** form of this command.

http client source-interface { **ipv4** | **ipv6** }

Syntax Description

ipv4 *ip-address*	Enter ipv4 address from interface.
ipv6 *ip-address*	Enter ipv6 address from interface.

Command Default

No default behavior or values.

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Command Modes

HTTP configuration

Usage Guidelines

Use the **http client source-interface** command to configure ipv4 and ipv6 source interfaces. If both the source interfaces are configured, then the source interface is selected depending on the host DNS resolution.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure ipv4 source interface for HTTP connection:

```
RP/0/RP0/CPU0:router(config)#http client source-interface ipv4 gigabitEthernet 0/0/0/0
```

The following example shows how to configure ipv6 source interface for HTTP connection:

```
RP/0/RP0/CPU0:router(config)#http client source-interface ipv6 gigabitEthernet 0/0/0/0
```

http client tcp-window-scale

To configure the TCP window scale factor for high latency links, use the **http client tcp-window-scale** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client tcp-window-scale *scale*

Syntax Description

scale	Specify the TCP window scale for HTTP requests. Range is 1 to 14.

Command Default

By default, TCP window scale is disabled.

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Command Modes

HTTP configuration

Usage Guidelines

Use this command to configure the TCP window scale for HTTP requests.



Note Currently, this is enabled for copying of files using HTTP.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to set the TCP window scale to 10:

```
RP/0/RP0/CPU0:router(config)#http client tcp-window-scale 10
```

http client version

To configure the HTTP version to be used for HTTP requests, use the **http client version** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client version *version*

Syntax Description		
	version*version*	Specify the HTTP version to be used for HTTP requests. Select one of the following versions: • **1.0** - Forces HTTP1.0 to be used for all HTTP requests. • **1.1** - Forces HTTP1.1 to be used for all HTTP requests. • **default** - libcurl picks up HTTP version automatically.

Command Default By default, libcurl does not force the HTTP version.

Note HTTP Client uses libcurl version 7.30

Command History	Release	Modification
	Release 7.10.1	This command was introduced.

Command Modes HTTP configuration

Usage Guidelines Use this command to configure the HTTP version to be used in HTTP requests.

Task ID	Task ID	Operations
	config-services	read, write

The following example shows how to configure the HTTP version to 1.1:

```
Router(config)#http client version 1.1
```

http client vrf

To configure a new VRF to be used by the HTTP client, use the **http client vrf** command. To remove the specified vrf, use the **no** form of this command.

http client vrf *vrf-name*

Syntax Description		
	vrf-name	Specifies the name of the VRF to be used by the HTTP client.

Command Default If not configured, the default VRF "default-vrf" will be used.

Command History	Release	Modification
	Release 7.10.1	This command was introduced.

Command Modes HTTP configuration

Usage Guidelines A HTTP client can have only one VRF. If a specific VRF is not configured for the HTTP client, the default VRF is assumed.

Task ID

Task ID	Operations
config-services	read, write

The following example shows the HTTP client being configured to start with the specified VRF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# http client vrf green
```

http-proxy

To configure the Call Home HTTP proxy server, use the **http-proxy** command in the call home profile configuration mode.

http-proxy *proxy-server-name* **port** *port-number*

Syntax Description

proxy-server-name	Specifies the name of the proxy server.
port-number	Specifies the port for the specified HTTP proxy server.

Command Default None

Command Modes Call home profile configuration mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines None

The following example configures the call home HTTP proxy server :

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#call-home
RP/0/RP0/CPU0:ios(config-call-home)#http-proxy aa.bbb.cc.dd port 100
```

hw-module

To configure the card in the module (muxponder), slice configuration (muxponder slice), or regen mode, use the **hw-module** command in Cisco IOS XR configuration mode.

hw-module location *location* { **mxponder | mxponder-slice** *mxponder-slice-number* { **trunk-mode [ZR | OR]** } } **client-rate [100GE | OTU4] trunk-rate [50G | 100G | 150G | 200G | 250G | 300G | 350G | 400G | 450G | 500G | 550G | 600G] [drop-lldp] [client-port-ains-soak hours** *hours* **minutes** *minutes*]
hw-module location *location* { **regen trunk-rate** *trunk-rate* **regen-slice** *slice-number* }
hw-module location *location* **mxponder arp-snoop**
hw-module location *location* **attention-led all-ports |** *port-number*
hw-module location *location* { **mxponder | mxponder-slice** *mxponder-slice-number* { **trunk-rate [100G | 200G | 300G | 400G]** { **client-type [100G | OTU4] | [client-port-rate [2-5] | [6-9]][client-type [100GE | OTU4]]** } } }

Syntax Description

location *location*	Specifies the location of the optics controller.
mxponder	Configures the card in muxponder mode.
mxponder-slice *mxponder-slice-number*	Configures the card in muxponder slice configuration. Slice numbers can be 0 or 1.
trunk-mode [ZR | OR]	Specifies the trunk mode when using a Bright ZR+ pluggable module as the trunk pluggable on a QXP card. Use ZR for ethernet and OR for OTN datapath.
client-rate [100GE | OTU4]	Specifies the traffic rate on the client ports. The supported client rates are 100GE and OTU4.
trunk-rate [50G | 100G | 150G | 200G | 250G | 300G | 350G | 400G | 450G | 500G | 550G | 600G]	Specifies the traffic rate on the trunk ports. The supported trunk rates are 150G, 200G, 250G, 300G, 350G, 400G, 450G, 500G, 550G, and 600G. From R7.2.1, you can configure trunk rates of 50G, 100G, and 150G to support Binary Phase-Shift Keying (BPSK) modulation. **Note** The 150G, 250G, 350G, 450G, and 550G data rates can be configured only in the muxponder card mode.
drop-lldp	Enables LLDP drop on a muxponder or muxponder slice.
client-port-ains-soak hours *hours* **minutes** *minutes*	Specifies the AINS configuration in hours and minutes.

regen trunk-rate *trunk-rate*	Configures the card in Regen mode. The supported trunk rates are 100G to 600G in multiples of 100G.
regen-slice*slice-number*	Specify the slice number on which you want to enable regen mode. The supported trunk rates are 100G to 400G in multiples of 100G. Valid values: • QXP Card: 0 to 5 (Only alternate slices can be configured.)
arp-snoop	Configures MAC address or ARP snoop on the client ports.
attention-ledall-ports | *port-number*	Turns on the attention LED on all the ports or on a specific port of the line card.
trunk-rate	Specifies the traffic rate on the trunk ports. The supported trunk rates is 100G, 200G, 300G, and 400G.
client-port-rate *client-port-number*	Specifies client port number. • Mxponder-slice 0—Client ports 2, 3, 4, and 5 are mapped to the trunk port 0. • Mxponder-slice 1—Client ports 6, 7, 8, and 9 are mapped to the trunk port 1.
client-type [100GE | OTU4]	Specifies the traffic type on the client ports. The supported client types are 100GE and OTU4.

Command Default

No slice is configured.

You must configure the card mode before enabling LLDP drop.

Command Modes

Cisco IOS XR Configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.1.1	**regen** keyword was added.
Release 7.2.1	**arp-snoop** keyword was added.

Release	Modification
Release 7.3.1	**trunk-rate 50G | 100G**keyword options are introduced.
Release 7.7.1	**attention-led** keyword was introduced.
Release 7.10.1	**regen-slice**, **client-port-rate [2-5] | [6-9]**, **client-type <100GE | OTU4>** , **trunk-mode [ZR | OR]** keywords were introduced.

Example

The following is a sample in which the card is configured in the muxponder mode with 100GE client payload and 500G trunk payload.

```
RP/0/RP0/CPU0:ios#configure
Sun Feb 24 14:09:33.989 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/2 mxponder client-rate 100GE
RP/0/RP0/CPU0:ios(config)#hw-module location 0/2 mxponder trunk-rate 500G
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the card is configured in the muxponder mode with a 550G trunk payload.

```
RP/0/RP0/CPU0:ios#config
Tue Oct 15 01:24:56.355 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder client-rate 100GE
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder trunk-rate 550G
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the card is configured in the muxponder mode with OTU4 client payload and 500G trunk payload.

```
RP/0/RP0/CPU0:ios#configure
Sun Feb 24 14:09:33.989 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/2 mxponder client-rate OTU4
RP/0/RP0/CPU0:ios(config)#hw-module location 0/2 mxponder trunk-rate 500G
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the card is configured in the muxponder slice 0 mode with a 300G trunk payload.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0 client-rate 100GE
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0 trunk-rate 300G
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the card is configured in the muxponder slice 1 mode with a 400G trunk payload.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 1 client-rate 100GE
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 1 trunk-rate 400G
RP/0/RP0/CPU0:ios(config)#commit
```

The following example shows how to configure LLDP drop on a muxponder slice.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0 drop-lldp
```

The following is a sample in which all the client ports are configured with AINS with soak time as 15 minutes.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/3 mxponder client-rate 100GE trunk-rate 500G
RP/0/RP0/CPU0:ios(config)#hw-module location 0/3 mxponder client-port-ains-soak hours 0
minutes 15
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample to configure the card in Regen mode.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/0
RP/0/RP0/CPU0:ios(config-hwmod)#regen
RP/0/RP0/CPU0:ios(config-regen)#trunk-rate 400
RP/0/RP0/CPU0:ios(config-regen)#commit
RP/0/RP0/CPU0:ios(config-regen)#exit
```

The following is a sample to configure regen mode on slices 0, 2, and 4 with a 400G trunk rate on each slice of the QXP card.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/3 regen-slice 0
RP/0/RP0/CPU0:ios(config-regen)#trunk-rate 400G
RP/0/RP0/CPU0:ios(config)#hw-module location 0/3 regen-slice 2
RP/0/RP0/CPU0:ios(config-regen)#trunk-rate 400G
RP/0/RP0/CPU0:ios(config)#hw-module location 0/3 regen-slice 4
RP/0/RP0/CPU0:ios(config-regen)#trunk-rate 400G
RP/0/RP0/CPU0:ios(config-regen)#commit
```

The following is a sample in which the 2-QDD-C card is configured with mixed client rates in the muxponder slice 1 and 0 modes.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 23 06:10:22.227 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0 client-rate OTU4 trunk-rate
 400G
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 1 client-rate 100GE trunk-rate
 400G
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the 2-QDD-C card is configured with mixed client rates in the same muxponder slice 0 mode.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 23 06:10:22.227 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0 client-port-rate 2
client-type OTU4 trunk-rate 400G
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0 client-port-rate 3
client-type 100GE trunk-rate 400G
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample to configure MAC address or ARP snoop on client ports for Mxponder mode configuration.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 16 19:08:17.154 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder arp-snoop
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample to configure MAC address snoop on client ports for slice mode configuration.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 16 19:30:33.933 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/3 mxponder-slice 0
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-rate 100GE
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#trunk-rate 600G
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#arp-snoop
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
Mon Mar 16 19:30:52.636 UTC
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#end
```

The following example shows how to configure trunk rate to 50G:

```
RP/0/RP0/CPU0:(config)#hw-module location 0/0 mxponder
RP/0/RP0/CPU0:(config-hwmod-mxp)#trunk-rate 50G
RP/0/RP0/CPU0:(config-hwmod-mxp)#commit
```

hw-module (OTN-XP Card)

To configure the OTN-XP card in the muxponder mode, use the **hw-module** command in IOS XR configuration mode.

hw-module location *location* **mxponder-slice** *mxponder-slice-number* **trunk-rate [100G | 200G | 300G | 400G] client-port-rate** *client-port-number* **lane** *lane number* **client-type [10GE | OTU2 | OTU2e | 400GE | FC16 | FC32 | oc192 | stm64]**
hw-module location *location* **attention-led all-ports |** *port-number*

Syntax Description

location *location*	Specifies the location of the optics controller.
mxponder-slice *mxponder-slice-number*	Configures the card in muxponder mode. The muxponder configuration supports two slices, 0 and 1.
protected	Enables the Automatic Protection System on the OTN XP card.
trunk-rate	Specifies the traffic rate on the trunk ports. The supported trunk rates is 100G, 200G, 300G, and 400G.

client-port-rate *client-port-number*	Specifies client port number. • Mxponder-slice 0—Client ports 4, 5, and 2 are mapped to the trunk port 0. • Mxponder-slice 1—Client ports 7, 6, and 11 are mapped to the trunk port 1.
lane *lane-number*	Specifies client port lane number.
client-type [10GE | OTU2 | OTU2e | 400GE | FC16 | FC32 | oc192 | stm64]	Specifies the traffic type on the client ports. The supported client types are 10GE, OTU2, OTU2e, FC16, FC32, OC192, STM64, and 400GE.
attention-ledall-ports | *port-number*	Turns on the attention LED on all the ports or on a specific port of the line card.

Command Default

None

Command Modes

Cisco IOS XR Configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.
Release 7.3.2	The trunk rates 200G, 300G and 400G were introduced.
Release 7.3.2	The client type 400GE was introduced.
Release 7.5.2	The client types FC16 and FC32 were introduced.
Release 7.7.1	**attention-led** keyword was introduced.
Release 7.10.1	The client types OC192 and STM64 were introduced.

The following is a sample in which the OTN-XP card is configured with mixed client rates in the mxponder-slice 0 mode.

```
RP/0/RP0/CPU0:ios#config
Tue Apr 21 09:21:44.460 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#trunk-rate 100G
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 2 lane 3 client-type OTU2
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 2 lane 4 client-type OTU2
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 4 lane 1 client-type 10GE
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
```

The following sample configures inverse muxponder for 400GE over 2x200G CFP2 trunk ports.

```
RP/0/RP0/CPU0:ios(config)#hw-module location 0/0 mxponder
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#trunk-rate 200G
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 client-type 400GE
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
```

The following sample configures 300G trunk rate on the OTN-XP card:.

```
RP/0/RP0/CPU0:ios#config
Wed Jun  2 17:17:59.409 UTC
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder-slice 0
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#trunk-rate 300G
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
```

The following is a sample to configure 16G FC muxponder mode on slice 0 of the OTN-XP card:.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/2 mxponder-slice 0
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#trunk-rate 400G
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 1 lane 1 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 1 lane 2 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 1 lane 3 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 1 lane 4 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 1 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 2 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 3 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 4 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 1 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 2 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 3 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 4 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 9 lane 1 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 9 lane 2 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 9 lane 3 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 9 lane 4 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 1 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 2 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 3 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 4 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 11 lane 1 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 11 lane 2 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 11 lane 3 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 11 lane 4 client-type fc16
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
Fri Feb 4 16:06:59.967 UTC
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#
```

The following is a sample to configure 32G FC muxponder mode on slice 0 of the OTN-XP card:

```
RP/0/RP0/CPU0:ios#configure
Fri Feb 4 16:24:53.964 UTC
RP/0/RP0/CPU0:ios(config)#
RP/0/RP0/CPU0:ios(config)#hw-module location 0/2 mxponder-slice 0
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#trunk-rate 400G
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 1 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 2 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 3 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 6 lane 4 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 1 client-type fc32
```

```
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 2 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 3 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 7 lane 4 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 1 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 2 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 3 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-port-rate 10 lane 4 client-type fc32
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
Fri Feb 4 16:26:46.550 UTC
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#
```

ikev2 policy

To specify an IKEv2 policy name, use the **ikev2 policy** command in configuration mode.

ikev2 policy *policy-name*

Syntax Description

policy-name	IKEv2 policy name upto 32 characters.

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 policy is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 19:26:45.752 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 policy mypolicy
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#proposal proposal1
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#match address local 10.0.0.1
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#commit
Thu Mar  7 19:29:25.043 UTC
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 policy mypolicy
Thu Mar  7 19:30:30.343 UTC

Policy Name                          : mypolicy
================================================================================
Total number of match local addr     : 1
   Match address local               : 10.0.0.1
--------------------------------------------------------------------------------
Total number of proposal attached    : 1
   Proposal Name                     : proposal1
```

ikev2 profile

To configure an IKEv2 profile, use the **ikev2 profile** command in configuration mode.

ikev2 profile *profile-name* **keyring ppk** *name*

Syntax Description

profile-name	Name of the IKEv2 profile.
keyring ppk	It specifies that ppk needs to be used and which keyring has the ppk configuration.
name	name of the keyring configured.

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.
Release 24.1.1	The key word keyring ppk was introduced.

Example

The following is a sample in which an IKEv2 profile is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 20:00:36.490 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 profile profile1
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#match identity remote address 10.0.0.1
255.255.255.0
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#keyring kyr1
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#lifetime 120
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#commit
Thu Mar  7 20:15:03.401 UTC
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 profile profile1
Thu Mar  7 20:15:25.776 UTC

Profile Name                          : profile1
================================================================================
Keyring                               : kyr1
Lifetime(Sec)                         : 120
DPD Interval(Sec)                     : 10
DPD Retry Interval(Sec)               : 2
Match ANY                             : NO
Total Match remote peers              : 1
   Addr/Prefix                        : 10.0.0.1/255.255.255.0
```

The following is a sample in which keyring ppk is specified in the IKEv2 profile.

```
RP/0/1/CPU0:ios(config)#ikev2 profile test
RP/0/1/CPU0:ios(config-ikev2-profile-test)#keyring dynamic
```

```
RP/0/1/CPU0:ios(config-ikev2-profile-test)#keyring ppk dynamic
RP/0/1/CPU0:ios(config-ikev2-profile-name)#match address 10.0.0.1 255.255.255.0
```

ikev2 proposal

To specify an IKEv2 proposal name, use the **ikev2 proposal** command in the configuration mode .

ikev2 proposal *proposal-name*

Syntax Description

proposal-name	Name of IKEv2 proposal upto 32 characters.

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 proposal is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 19:19:30.259 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 proposal proposal1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#encryption aes-cbc-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#integrity sha-1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#prf sha-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#dh 20
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#commit
Thu Mar  7 19:20:30.916 UTC
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 proposal proposal1
Thu Mar  7 19:20:48.929 UTC

Proposal Name              : proposal1
================================================================================
Status                     : Complete
--------------------------------------------------------------------------------
Total Number of Enc. Alg.  : 1
   Encr. Alg.              : CBC-AES-256
--------------------------------------------------------------------------------
Total Number of Hash. Alg. : 1
   Hash. Alg.              : SHA 1
--------------------------------------------------------------------------------
Total Number of PRF. Alg.  : 1
   PRF. Alg.               : SHA 256
--------------------------------------------------------------------------------
Total Number of DH Group   : 1
   DH Group                : Group 20
```

integrity

To specify one or more transforms of the integrity algorithm type, use the **integrity** command in IKEv2 proposal configuration mode.

integrity *algorithm-type*

Syntax Description

algorithm-type	Integrity algorithm type. The possible values are: sha-1, sha-256, sha-384, and sha-512.

Command Default

None

Command Modes

IKEv2 proposal configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 proposal is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 19:19:30.259 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 proposal proposal1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#encryption aes-cbc-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#integrity sha-1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#prf sha-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#dh 20
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#commit
Thu Mar  7 19:20:30.916 UTC
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 proposal proposal1
Thu Mar  7 19:20:48.929 UTC

Proposal Name              : proposal1
================================================================================
Status                     : Complete
--------------------------------------------------------------------------------
Total Number of Enc. Alg.  : 1
   Encr. Alg.              : CBC-AES-256
--------------------------------------------------------------------------------

Total Number of Hash. Alg. : 1
   Hash. Alg.              : SHA 1

--------------------------------------------------------------------------------
Total Number of PRF. Alg.  : 1
   PRF. Alg.               : SHA 256
--------------------------------------------------------------------------------
Total Number of DH Group   : 1
   DH Group                : Group 20
```

interface gcc0

To configure the GCC0 interface, use the **interface gcc0** command in configuration mode.

interface gcc0 *R/S/I/P*

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port of the GCC0 interface.

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.1.1	This command is introduced.

Example

The following is a sample to configure the GCC0 interface using the static IP address.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#interface gcc0 0/1/0/0
P/0/RP0/CPU0:ios(config-if)#ipv4 address 10.1.1.1 255.255.255.0
RP/0/RP0/CPU0:ios(config-if)#commit
RP/0/RP0/CPU0:ios(config-if)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show run interface gcc0 0/1/0/0
interface GCC00/1/0/0
ipv4 address 10.1.1.1 255.255.255.0
!
```

The following is a sample to configure the GCC0 interface using the loopback IP address.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:R2(config)#interface gcc0 0/1/0/0
RP/0/RP0/CPU0:R2(config-if)#ipv4 unnumbered loopback 0
RP/0/RP0/CPU0:ios(config-if)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

interface gcc2

To configure the GCC2 interface, use the **interface gcc2** command in configuration mode.

interface gcc2 *R/S/I/P/L*

Syntax Description

R/S/I/P/L	Rack/Slot/Instance/Port/Lane of the GCC2 interface.

Command Default None

Command Modes Configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample to configure the GCC2 interface using the static IP address.

```
RP/0/RP0/CPU0:ios#config
Tue Mar 12 11:16:04.749 UTC
RP/0/RP0/CPU0:ios(config)#interface gcc2 0/1/0/0/1
P/0/RP0/CPU0:ios(config-if)#ipv4 address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:ios(config-if)#commit
Tue Mar 12 11:18:32.867 UTC
RP/0/RP0/CPU0:ios(config-if)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show run interface gcc2 0/1/0/0/1
Tue Mar 12 11:19:00.475 UTC
interface gcc2 0/1/0/0/1
 ipv4 address 10.0.0.1 255.255.255.0
!
```

The following is a sample to configure the GCC2 interface using the loopback IP address.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:R2(config)#interface gcc2 0/1/0/0/1
RP/0/RP0/CPU0:R2(config-if)#ipv4 unnumbered loopback 0
RP/0/RP0/CPU0:ios(config-if)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

ipcc routed

To specify the LMP neighbor IPCC configuration for GMPLS UNI, use the **ipcc routed** command in the neighbor sub-mode for LMP GMPLS-UNI controller configuration mode.

ipcc routed

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes LMP GMPLS-UNI controller neighbor configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines The LMP submode enables GMPLS-UNI LMP functionality and acts as a container for other GMPLS-UNI LMP configuration commands.

Example

The following example shows how to specify the IPCC configuration for the GMPLS UNI controller 0/0/0/0, neighbor UN02.

```
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#neighbor UN02
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-nbr-UN02)#ipcc routed
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-nbr-UN02)#
```

ipv4 access-group

To configure the Access List (ACL), use the **ipv4 access-group** command at the IPv4 interface in the interface configuration mode.

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

Syntax Description

access-list-name	Access list name. Names cannot contain a space or quotation marks.
ingress	Specifies an inbound interface.
egress	Specifies an outbound interface.

Command Default No IPv4 access list is defined.

Command Modes Interface configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines Use the ipv4 access-list command to configure an IPv4 access list. This command places the system in access list configuration mode, in which the denied or permitted access conditions must be defined with the deny or permit command.

Example

The following examples shows how to configure the Access List at the IPv4 interface in the configuration mode:

```
interface MgmtEth0/RP0/CPU0/0
ipv4 address 10.1.1.1 255.255.255.0
ipv4 access-group IPV4_ICMP_DENY ingress
ipv4 access-group IPV4_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
!
```

ipv6 access-group

To configure the Access List (ACL), use the **ipv6 access-group** command at the IPv6 interface in the interface configuration mode.

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

Syntax Description

access-list-name	Access list name. Names cannot contain a space or quotation marks.
ingress	Specifies an inbound interface.
egress	Specifies an outbound interface.

Command Default

No IPv6 access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines

Use the ipv6 access-list command to configure an IPv6access list. This command places the system in access list configuration mode, in which the denied or permitted access conditions must be defined with the deny or permit command.

Example

The following examples shows how to configure the Access List at the IPv6 interface in the configuration mode

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

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
!
```

key config-key password-encryption

To create a primary key for the Type 6 password encryption feature, use the **key config-key password-encryption** command in EXEC mode.

key config-key password-encryption [**delete**]

Syntax Description

delete	(Optional) Deletes the primary key for Type 6 password encryption.

Command Default

No primary key exists.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XR Release 7.0.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to create a primary key for Type 6 password encryption:

```
P/0/0/CPU0:ios#key config-key password-encryption
Thu Jul 11 09:40:47.396 UTC
New password Requirements: Min-length 6, Max-length 64
Enter new key :
Enter confirm key :
Master key operation is started in background
```

keyring

To configure the details of the IKEv2 keyring that consists of the preshared keys along with the IP address for IKEv2 negotiations used to establish the peer tunnel, use the **keyring** command in XR Config mode.

keyring peer *name* **ppk** { **manual | dynamic** } [**required**] { **address** *ipv4 mask* **pre-shared-key** { **clear** *clear-text key* | **local** *local key* | **password** *encrypted key* | **password 6** *encrypted key* }

Syntax Description

keyring-name	Name of the keyring upto 32 characters.
peer *name*	Specifies the name of the peer interface

ppk [dynamic | manual]	Specifies whether the Postquantum Preshared Keys (PPK) is dynamic or manual.
address *ipv4 mask*	Specifies the ip address of the peer interface along with the mask.
pre-shared-key	Configures the preshared keys for authentication.
clear *clear-text key*	Specifies that the preshared key is in cleartext format.
local *local key*	Specifies that the preshared key is a local passphrase.
password *encrypted key*	Specifies that the preshared key is an encrypted string in hexadecimal format.
password 6 *encrypted key*	Specifies that the preshared key is an encrypted string in hexadecimal format. The preshared keystring will be stored in an encoded format when password6 is enabled.
required	Specifies whether dynamic or manual ppk configuration is mandatory or not.

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.
Release 24.1.1	The keyword ppk [dynamic | manual] was introduced.
Release 24.3.1	The keyword password6 was introduced.

Example 1

The following is a sample in which a keyring is configured.

```
RP/0/RP0/CPU0:ios#conf
Thu Mar  7 19:33:14.594 UTC
RP/0/RP0/CPU0:ios(config)#keyring kyr1
RP/0/RP0/CPU0:ios(config-keyring-kyr1)#peer peer1
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#pre-shared-key password 14341B180F547B7977
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#commit
Thu Mar  7 19:54:33.314 UTC
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#exit
RP/0/RP0/CPU0:ios(config-keyring-kyr1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show keyring kyr1
Thu Mar  7 19:58:07.135 UTC

Keyring Name                          : kyr1
================================================================================
Total Peers                           : 1
--------------------------------------------------------------------------------
   Peer Name                          : peer1
   IP Address                         : 10.0.0.1
   Subnet Mask                        : 255.255.255.0
```

```
   Local PSK                          : Configured
   Remote PSK                         : Configured
```

Example 2

The following is a sample in which the dynamic ppk is configured.

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RP0/CPU0:ios(config)#keyring dynamic
RP/0/RP0/CPU0:ios(config-ikev2-keyring)#peer peer1
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#ppk dynamic qkd required
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#pre-shared-key cisco123!cisco123
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#address 10.0.0.1 255.0.0.0

RP/0/1/CPU0:ios(config)#ikev2 profile test
RP/0/1/CPU0:ios(config-ikev2-profile-test)#keyring dynamic
RP/0/1/CPU0:ios(config-ikev2-profile-test)#keyring ppk dynamic
RP/0/1/CPU0:ios(config-ikev2-profile-test)#match address 10.0.0.1 255.255.255.0
```

Example 3

The following is a sample in which the manual ppk is configured.

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RP0/CPU0:ios(config)#keyring manual
RP/0/RP0/CPU0:ios(config-ikev2-keyring)#peer peer1
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#ppk manual id cisco123 key password
070804564A41694B89 required
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#pre-shared-key cisco123!cisco123
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#address 10.0.0.1 255.0.0.0
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#exit
RP/0/RP0/CPU0:ios(config)#exit

RP/0/1/CPU0:ios(config)#ikev2 profile test
RP/0/1/CPU0:ios(config-ikev2-profile-test)#keyring manual
RP/0/1/CPU0:ios(config-ikev2-profile-test)#keyring ppk manual
RP/0/1/CPU0:ios(config-ikev2-profile-test)#match address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:ios(config-ikev2-profile-test)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

Example 4

These are the examples where the PPK and preshared key are configured with the `password6` keyword, after enabling the Type 6 method:

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RP0/CPU0:ios(config)#keyring type6_psk
RP/0/RP0/CPU0:ios(config-ikev2-keyring)#peer peer1
RP/0/RP0/CPU0:ios(config-ikev2-keyring)#pre-shared-key
password6
525548665b4e534660504c54645d63526668604945635a6452604a5f644d605a5c4461644d4e444e6566414142
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#address 10.0.0.1 255.0.0.0
```

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RP0/CPU0:ios(config)#keyring type6_ppk
RP/0/RP0/CPU0:ios(config-ikev2-keyring)#peer peer1
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#ppk manual id 123 key password6
 426447414e60494d48655d434f4749525d69484f434d445850675258544d56444a5d4d5b664b4c55624e414142
```

```
 required
RP/0/RP0/CPU0:ios(config-ikev2-keyring)#pre-shared-key
```

lc-module (OTN-XP Card)

To configure the LC mode on the OTN-XP card, use the **lc-module** command in IOS XR configuration mode.

lc-module location *location* **lcmode** *mode*

Syntax Description

location *location*	Specifies the location of the optics controller.
lcmode *mode*	Configures the line card mode. The LC modes supported on the OTN-XP card are: • 10G-GREY-MXP • 40x10G-4x100G-MXP • 4x100G-MXP-400G-TXP • FC-MXP • OTUCn-REGEN **Note** Only 10G-GREY-MXP is supported in Release 7.2.1 even though all the above modes are software configurable.

Command Default

None

Command Modes

Cisco IOS XR Configuration

Command History

Release	Modification
Release 7.2.1	This command was introduced.
Release 7.5.2	The LC modes FC-MXP and OTUCn-REGEN were introduced.

Example

The following is a sample in which the OTN-XP card is configured in the 10G-GREY-MXP mode.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar 26 21:40:51.495 UTC
```

```
RP/0/RP0/CPU0:ios(config)#lc-module location 0/1 lcmode 10G-GREY-MXP
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the OTN-XP card is configured in the FC-MXP mode.

```
RP/0/RP0/CPU0:ios#configure
Fri Feb  4 16:06:59.967 UTC
RP/0/RP0/CPU0:ios(config)#lc-module location 0/1 lcmode FC-MXP
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which the OTN-XP card is configured in the OTUCn-REGEN mode.

```
RP/0/RP0/CPU0:ios#configure
Fri Feb  4 16:06:59.967 UTC
RP/0/RP0/CPU0:ios(config)#lc-module location 0/1 lcmode OTUCn-REGEN
RP/0/RP0/CPU0:ios(config)#commit
```

license smart register

To register the device instance with Cisco licensing cloud, use the **license smart register idtoken** *token-id* **force** command.

license smart register idtoken *token-id* [**force**]

Syntax Description

token_id	Specifies the token generated in smart manager.
force	If the registration fails due to communication failure between the device and the portal or satellite, the system waits for 24 hours before attempting to register the device again. Use this option to force the registration.

Command Default

None

Command Modes

None

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Use this command to register the device instance with Cisco licensing cloud.

The following example registers and sets the token ID required for registration of NCS 1004.

```
RP/0/RP0/CPU0:ios#license smart register token-id
```

license smart renew

To manually renew the ID certification or authorization, use the **license smart renew** command.

license smart renew id { **ID**|**auth** }

Syntax Description

ID	ID certificates are renewed automatically after six months. In case, the renewal fails, the product instance goes into unidentified state. You can manually renew the ID certificate using this option.
auth	Authorization periods are renewed by the Smart Licensing system every 30 days. As long as the license is in an 'Authorized' or 'Out-of-compliance' (OOC), the authorization period is renewed. Use this command to make an on-demand manual update of your registration. Thus, instead of waiting 30 days for the next registration renewal cycle, you can use this option to instantly find out the status of your license. After 90 days, the authorization period expires and the status of the associated licenses display "AUTH EXPIRED". Use this option to retry the authorization period renewal. If the retry is successful, a new authorization period begins.

Command Default None

Command Modes None

Command History

Release	Modification
R7.0.1	This command was introduced.

Usage Guidelines None

The following example manually renews the ID certificate for NCS 1004.

```
RP/0/RP0/CPU0:ios#license smart renew id
```

The following example manually renews the authorization for NCS 1004.

```
RP/0/RP0/CPU0:ios#license smart renew auth
```

license smart deregister

To cancel the registration of your device, use the **license smart deregister** command.

license smart deregister

Command Default None

Command Modes None

Command History

Release	Modification
R7.0.1	This command was introduced.

Usage Guidelines

When your device is taken off the inventory, shipped elsewhere for redeployment or returned to Cisco for replacement using the return merchandise authorization (RMA) process, you can use this command to cancel the registration on your device. All smart licensing entitlements and certificates on the platform are removed.

The following example deregisters NCS 1004.

```
RP/0/RP0/CPU0:ios#license smart deregister
```

lifetime

To configure the lifetime of IKEv2 security association (SA), use the **lifetime** command in IKEv2 profile configuration mode.

lifetime *seconds*

Syntax Description

seconds	Specifies the lifetime in seconds. The range is from 120 to 86400 seconds.

Command Default

None

Command Modes

IKEv2 profile configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 profile is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 20:00:36.490 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 profile profile1
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#match identity remote address 10.0.0.1
255.255.255.0
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#keyring kyr1
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#lifetime 120
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#commit
Thu Mar  7 20:15:03.401 UTC
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 profile profile1
Thu Mar  7 20:15:25.776 UTC

Profile Name                          : profile1
================================================================================
Keyring                               : kyr1
Lifetime(Sec)                         : 120
DPD Interval(Sec)                     : 10
DPD Retry Interval(Sec)               : 2
Match ANY                             : NO
Total Match remote peers              : 1
   Addr/Prefix                        : 10.0.0.1/255.255.255.0
```

link-id ipv4 unicast

To specify the local optical interface address for an LMP link for a GMPLS UNI controller, use the **link-id ipv4 unicast** command in GMPLS-UNI controller configuration mode.

link-id ipv4 unicast *address*

Syntax Description

address	Specifies the optical unicast IPv4 address.

Command Default

None

Command Modes

LMP GMPLS-UNI controller configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to specify the local optical interface address for an LMP link.

```
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-ctrl)#link-id ipv4 unicast 10.11.1.1
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-ctrl)#
```

linux security audit

To enable the Linux audit monitoring and logging capabilities, use the linux security audit command in XR Config mode.

linux security audit **monitor** { `all` | `authlog-files` | `cron-files` | `dns-client-files` | `docker` | `file-deletion` | `file-perm-changes` | `kernel-module-mgmt` | `process-audits` | `system-login-reboot` | `system-software` | `system-time-change` | `user-group-config-files` | `user-privilege-mgmt` | `xr-software` } | **logging syslog** }

Syntax Description

monitor	Enable audit monitoring.
all	Enable audit monitoring for all rule groups.
authlog-files	Enable audit monitoring for changes in authlog files.
cron-files	Enable audit monitoring for changes in cron files.

dns-client-files	Enable audit monitoring for changes in DNS client files.
docker	Enable audit monitoring for changes in docker.
file-deletion	Enable audit monitoring for file deletion.
file-perm-changes	Enable audit monitoring for changes in file permissions.
kernel-module-mgmt	Enable audit monitoring for kernel module management.
process-audits	Enable audit monitoring for process audits.
system-login-reboot	Enable audit monitoring for system login and reboot.
system-software	Enable audit monitoring for changes in system software.
system-time-change	Enable audit monitoring for changes in system time.
user-group-config-files	Enable auditmonitoring for changes in user group configuration files.
user-privilege-mgmt	Enable audit monitoring for changes in user privileges.
xr-software	Enable audit monitoring for changes in IOS XR software.
logging syslog	Enable forwarding of audit logs to a remote syslog server.

Command Default

Audit monitoring is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

Follow these guidelines for audit monitoring:

- Use caution when enabling **all** rule groups, especially those that monitor frequent events, as this may increase CPU, memory, or disk usage. Enable only the groups required for compliance or security needs.
- The RP/0/RP0/CPU0:ios stores audit logs locally at **/var/log/audit/audit.log** , unless you enable log forwarding.

Example

This example shows how you can enable audit monitoring with the **linux security audit monitor** command.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)# linux security audit monitor xr-software
RP/0/RP0/CPU0:ios(config)# linux security audit monitor user-group-config-files
RP/0/RP0/CPU0:ios(config)# commit
```

This example shows how you can enable audit log forwarding with the **linux security audit logging syslog** command.

```
RP/0/RP0/CPU0:ios# config
RP/0/RP0/CPU0:ios(config)# linux security audit logging syslog
RP/0/RP0/CPU0:ios(config)# logging 10.0.1.2 vrf default severity info port default facility
 local6
RP/0/RP0/CPU0:ios(config)# commit
```

lmp

To enable functionality for GMPLS UNI LMP and enter LMP configuration commands, use the **lmp** command in global configuration mode.

lmp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to enable LMP functionality and enter the sub-mode for LMP configuration commands.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#
```

match address local

To specify the IP address of the local node, use the **match address local** command in the IKEv2 policy configuration mode.

match address local *ipv4-address*

Syntax Description

ipv4-address	IP address of the local node.

Command Default

None

Command Modes IKEv2 policy configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 policy is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 19:26:45.752 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 policy mypolicy
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#proposal proposal1
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#match address local 10.0.0.1
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#commit
Thu Mar  7 19:29:25.043 UTC
RP/0/RP0/CPU0:ios(config-ikev2-policy-mypolicy)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 policy mypolicy
Thu Mar  7 19:30:30.343 UTC

Policy Name                           : mypolicy
================================================================================

Total number of match local addr      : 1
   Match address local                : 10.0.0.1

--------------------------------------------------------------------------------
Total number of proposal attached     : 1
   Proposal Name                      : proposal1
```

match identity remote address

To specify the IP address of the remote node, use the **match identity remote address** command in IKEv2 profile configuration mode.

match identity remote address { *ipv4-address* [*subnet-mask*] }

Syntax Description

ipv4-address	IP address of the remote node.
subnet-mask	Subnet mask address.

Command Default None

Command Modes IKEv2 profile configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 profile is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 20:00:36.490 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 profile profile1
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#match identity remote address 10.0.0.1
255.255.255.0

RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#keyring kyr1
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#lifetime 120
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#commit
Thu Mar  7 20:15:03.401 UTC
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 profile profile1
Thu Mar  7 20:15:25.776 UTC

Profile Name                          : profile1
================================================================================
Keyring                               : kyr1
Lifetime(Sec)                         : 120
DPD Interval(Sec)                     : 10
DPD Retry Interval(Sec)               : 2
Match ANY                             : NO
Total Match remote peers              : 1
   Addr/Prefix                        : 10.0.0.1/255.255.255.0
```

neighbor interface-id unnumbered

To specify the neighbor's optical interface ID of an LMP link for a GMPLS UNI controller, use the **neighbor interface-id unnumbered** command in GMPLS-UNI controller configuration mode.

neighbor interface-id unnumbered *interface-id*

Syntax Description

interface-id	Specifies the optical interface ID of the neighbor.

Command Default

None

Command Modes

LMP GMPLS-UNI controller configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to specify the optical interface ID of an LMP neighbor.

```
RP/0/RP0/CPU0:ios(config)#lmp
```

```
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-ctrl)#neighbor interface-id unnumbered 2130706976
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-ctrl)#
```

neighbor link-id ipv4 unicast

To specify the neighbor's optical address of an LMP link for a GMPLS UNI controller, use the **neighbor link-id ipv4 unicast** command in GMPLS-UNI controller configuration mode.

neighbor link-id ipv4 unicast *address*

Syntax Description

address	Specifies the IPv4 address of the neighbor.

Command Default

None

Command Modes

LMP GMPLS-UNI controller configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to specify the optical IPv4 address (10.1.1.1) of an LMP neighbor for controller 0/0/0/0:

```
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-ctrl)#neighbor link-id ipv4 unicast 10.1.1.1
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-ctrl)#
```

neighbor

To specify an LMP neighbor for GMPLS and enter commands to configure the neighbor, use the **neighbor** command in the LMP GMPLS-UNI configuration mode.

neighbor *name*

Syntax Description

name	Specifies the name of the LMP neighbor.

Command Default

None

Command Modes

LMP GMPLS-UNI configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines

Under the LMP GMPLS UNI submode, this command creates a submode in which other properties of the neighbor can be specified.

Example

The following example shows how to specify the neighbor UN01 for the GMPLS-UNI controller 0/0/0/0.

```
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#neighbor UN01
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-nbr-UN01)#exit
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-cntl)#neighbor UN01
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-cntl)#
```

nvgen default-sanitize

To enable sanitizing passwords in the output for **show running configurations** command, use the **nvgen default-sanitize** command.

nvgen default-sanitize { **password** }

Syntax Description

password	Removes the passwords in the running configuration and replaces it with the **<removed>** phrase.

Command Default

The output for the **show running configurations** command includes sensitive information such as passwords.

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XR Release 7.0.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to sanitize show running configurations:

```
RP/0/0/CPU0:ios(config)#nvgen-default-sanitize passwords
RP/0/0/CPU0:ios(config)#commit
```

otnsec policy

To configure an OTNSec policy, use the **otnsec policy** command in the configuration mode.

otnsec policy *policy-name*

Syntax Description

policy-name	Policy name

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an OTNSec policy is configured.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 11 15:16:58.417 UTC
RP/0/RP0/CPU0:ios(config)#otnsec policy otnsec-policy1
RP/0/RP0/CPU0:ios(config-otnsec-policy)#cipher-suite AES-GCM-256
RP/0/RP0/CPU0:ios(config-otnsec-policy)#security-policy must-secure
RP/0/RP0/CPU0:ios(config-otnsec-policy)#sak-rekey-interval 120
RP/0/RP0/CPU0:ios(config-otnsec-policy)#commit
```

The following is a sample of an OTNSec policy.

```
RP/0/RP0/CPU0:ios#show run otnsec policy otnsec-policy1
Tue Mar 12 11:14:03.591 UTC
otnsec policy otnsec-policy1
 cipher-suite AES-GCM-256
 security-policy must-secure
 sak-rekey-interval 120
!
```

password6 aes encryption

To enable a type 6 encrypted preshared key, use the **password encryption aes** command in global configuration mode.

password6 aes encryption

Syntax Description

This command has no arguments or keywords.

Command Default None

Command Modes Config mode

Command History

Release	Modification
Cisco IOS XR Release 7.0.1	This command was introduced.

Usage Guidelines You can securely store plain text passwords in type 6 format in NVRAM using a CLI. Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encrypt** command along with the **password encryption aes** command to configure and enable the password.

Example

he following example shows how a type 6 encrypted preshared key is enabled:

```
RP/0/RP0/CPU0:ios(config)#password6 encryption aes
```

path-option

To specify a path option for a GMPLS UNI tunnel, use the **path-option** command in GMPLS UNI controller tunnel-properties configuration sub-mode.

path-option 10 { no-ero | explicit { name *path-name* **| index** *index* **} } [xro-attribute-set** *name* **] [lockdown] [verbatim]**

Syntax Description

10	Specifies the path option index. 10 is the only supported index
explicit	Specifies that LSP paths are IP explicit paths.
name *path-name*	Specifies the path name of the IP explicit path.
no-ero	Specifies that no ERO object is included in signalling.
xro-attribute-set	(Optional) Specifies the xro attribute set for the path option.
name	Specifies the name of the xro-attribute-set.
lockdown	(Optional) Indicates that the tunnel does not reoptimize without user intervention.
verbatim	(Optional) Bypasses the topology check for explicit paths.

Command Default None

Command Modes GMPLS UNI controller tunnel-properties configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to specify the tunnel path option for controller 0/0/0/0, attribute set A01..

```
RP/0/RP0/CPU0:ios(config)#mpls traffic-eng
RP/0/RP0/CPU0:ios(config-mpls-te)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-te-gmpls)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-te-gmpls-cntl)#tunnel-properties
RP/0/RP0/CPU0:ios(config-te-gmpls-tun)#path-option 10 no-ero xro-attribute-set A01 lockdown
RP/0/RP0/CPU0:ios(config-te-gmpls-tun)#
```

peer

To specify the peer node during keyring configuration, use the **peer** command in keyring configuration mode.

peer *peer-name*

Syntax Description

peer-name	Peer node name.

Command Default

None

Command Modes

Keyring configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which a keyring is configured.

```
RP/0/RP0/CPU0:ios#conf
Thu Mar  7 19:33:14.594 UTC
RP/0/RP0/CPU0:ios(config)#keyring kyr1
RP/0/RP0/CPU0:ios(config-keyring-kyr1)#peer peer1
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#pre-shared-key key1|clear
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#commit
Thu Mar  7 19:54:33.314 UTC
RP/0/RP0/CPU0:ios(config-keyring-kyr1-peer-peer1)#exit
RP/0/RP0/CPU0:ios(config-keyring-kyr1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show keyring kyr1
```

```
Thu Mar  7 19:58:07.135 UTC

Keyring Name                          : kyr1
================================================================================
Total Peers                           : 1
--------------------------------------------------------------------------------

   Peer Name                          : peer1

   IP Address                         : 10.0.0.1
   Subnet Mask                        : 255.255.255.0
   Local PSK                          : Configured
   Remote PSK                         : Configured
```

pki trustpoint

To specify the trustpoints for use with the RSA signature authentication method, use the **pki trustpoint** command in IKEv2 profile configuration mode

pki trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Specifies the name of the trustpoint.

Command Default

None

Command Modes

IKEv2 profile configuration

Command History

Release	Modification
R7.2.1	This command was introduced.

Example

The following example shows how to specify the authentication mode in the IKEv2 profile.

```
RP/0/RP0/CPU0:ios#configure
Thu May 7 16:22:33.804 IST
RP/0/RP0/CPU0:ios(config)#ikev2 profile IP1
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#match identity remote address 10.1.1.2
255.255.255.255
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#pki trustpoint myca
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#lifetime 120
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#authentication local rsa-signature
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#authentication remote rsa-signature
RP/0/RP0/CPU0:ios(config-ikev2-profile-IP1)#commit
```

pm

To configure the performance monitoring parameters of the optics, Ethernet, and coherent DSP controllers, use the **pm** command in the controller configuration mode.

pm [**15-min | 30-sec | 24-hour**] [**optics** | **ether** | **pcs** | **fec** | **otn**] [**report | threshold**] *value*

Syntax Description

15-min | 30-sec | 24-hour	Configures performance monitoring parameters for 15 minute or 30 second or 24 hour intervals.
optics | **ether** | **pcs** | **fec** | **otn**	Specifies whether to configure performance monitoring parameters for the optics, Ethernet, or coherent DSP controllers.
report	Configures optics TCA reporting status.
threshold	Configures threshold on optics parameters.
value	Value of the reporting or threshold parameters.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The following table describes the optics PM parameters.

Parameter	Description
cd	Chromatic dispersion TCA reporting status or threshold
dgd	Differential group delay TCA reporting status or threshold
lbc	lbc TCA reporting status or threshold
lbc-pc	lbc percentage TCA reporting status or threshold
low-freq-off	low signal frequency offset TCA reporting status or threshold
opr	opr/opr-dbm TCA reporting status or threshold
opt	opt/opt-dbm TCA reporting status or threshold
osnr	Optical Signal to Noise Ratio TCA reporting status or threshold
pcr	Polarization Change Rate TCA reporting status or threshold
pdl	Polarization Dependent Loss TCA reporting status or threshold
pn	Phase Noise TCA reporting status or threshold
rx-sig-pow	rx signal power TCA reporting status or threshold
sopmd	Second Order Polarization Mode Dispersion TCA reporting status or threshold

The following table describes the OTN PM parameters.

Parameter	Description
ES-NE	Error seconds in the near end
ESR-NE	Error seconds ratio in the near end
SES-NE	Severely error seconds in the near end
SESR-NE	Severely error seconds ratio in the near end
UAS-NE	Unavailable seconds in the near end
BBE-NE	Background block errors in the near end
BBER-NE	Background block errors ratio in the near end
FC-NE	Failure counts in the near end
ES-FE	Error seconds in the far end
ESR-FE	Error seconds ratio in the far end
SES-FE	Severely error seconds in the far end
SESR-FE	Severely error seconds ratio in the far end
UAS-FE	Unavailable seconds in the far end
BBE-FE	Background block errors in the far end
BBER-FE	Background block errors ratio in the far end
FC-FE	Failure counts in the far end

The following table describes the Ethernet PM parameters.

Parameter	Description
rx-util	Bandwidth utilization of port at the ingress side in percentage.
tx-util	Bandwidth utilization of port at egress side in percentage.
rx-pkt	Number of received packets
stat-pkt	Status of received packets
octet-stat	Total number of octets of data received in the network
oversize-pkt	Total number of packets received that were longer than 1518 octets and were otherwise well formed
jabber-stats	Total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)

Parameter	Description
in-64-octets	Total number of packets received that were 64 octets in length
in-65-127-octets	Total number of packets received that were between 65 and 127 octets in length
in-128-255-octets	Total number of packets received that were between 128 and 255 octets in length
in-256-511-octets	Total number of packets received that were between 256 and 511 octets in length
in-512-1023-octets	Total number of packets received that were between 512 and 1023 octets in length
in-1024-1518-octets	Total number of packets received that were between 1024 and 1518 octets in length
in-mcast	Total number of multicast frames received error-free
in-bcast	Total number of broadcast frames received error-free
out-bcast	Total number of broadcast frames transmitted error-free
out-mcast	Total number of multicast frames transmitted error-free
tx-pkt	Number of transmitted packets
out-octets	Total number of octets transmitted out of the interface, including framing characters
ether-stat-multicast-pkt	Status of multicast packets
ether-stat-broadcast-pkt	Status of broadcast packets
ether-stat-undersized-pkt	Number of good packets received that are shorter than 64 bytes.
in-error-fragments	Number of bad packets received that are shorter than 64 bytes.
tx-undersized-pkt	Total number of packets transmitted that are shorter than 64 bytes.
tx-oversized-pkt	Total number of oversized packets transmitted.
tx-fragments	Total number of fragmented packets transmitted.
tx-jabber	Total number of Jabber packets transmitted.
tx-bad-fcs	Total number of bad FCS packets transmitted.
fcs-err	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
ifIn-Octets	Total number of octets received on the interface, including framing characters.
ifIn-errors	Number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.

Parameter	Description
in-good-bytes	Total number of good bytes or octets received.
in-good-pkts	Total number of good packets received.
long-frame	A count of frames received on a particular interface that exceed the maximum permitted frame size.
out-good-bytes	Total number of good bytes or octets transmitted
out-good-pkts	Total number of good packets transmitted.
1024-1518-octets	Total number of packets (including error packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
128-255-octets	Total number of packets (including error packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511-octets	Total number of packets (including error packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023-octets	Total number of packets (including error packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
64-octets	Total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127-octets	Total number of packets (including error packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

The following table describes the FEC PM parameters.

Parameter	Description
ec-words	Number of bit errors that are corrected by the system
uc-words	Number of words that are not corrected by the system

The following table describes the PCS PM parameters.

Parameter	Description
PCS-ES	Error seconds
PCS-SES	Severly error seconds
PCS-UAS	Unavailable seconds
PCS-ES-FE	Error seconds in far end

Parameter	Description
PCS-SES-FE	Severly error seconds in far end
PCS-UAS-FE	Unavailable seconds in far end

Example

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

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller optics 0/0/1/1 pm 24-hour optics threshold osnr max
345
RP/0/RP0/CPU0:ios(config)#commit
```

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

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller HundredGigECtrlr 0/3/0/2 pm 15-min pcs report bip
enable
RP/0/RP0/CPU0:ios(config)#commit
```

The following is a sample in which performance monitoring parameters of Coherent DSP controller is configured in 30 second intervals.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller coherentDSP 0/0/1/1 pm 30-sec fec threshold post-fec-ber
 max OE-15
RP/0/RP0/CPU0:ios(config)#commit
```

prf

To specify the Pseudo-Random Function (PRF) algorithm type, use the **prf** command in IKEv2 proposal configuration mode.

prf *prf-algorithm*

Syntax Description

prf-algorithm	PRF algorithm type. The possible values are sha-1, sha-256, sha-384, and sha-512.

Command Default

None

Command Modes

IKEv2 proposal configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an IKEv2 proposal is configured.

```
RP/0/RP0/CPU0:ios#configure
Thu Mar  7 19:19:30.259 UTC
RP/0/RP0/CPU0:ios(config)#ikev2 proposal proposal1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#encryption aes-cbc-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#integrity sha-1
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#prf sha-256
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#dh 20
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#commit
Thu Mar  7 19:20:30.916 UTC
RP/0/RP0/CPU0:ios(config-ikev2-proposal-proposal1)#exit
RP/0/RP0/CPU0:ios(config)#exit
RP/0/RP0/CPU0:ios#show ikev2 proposal proposal1
Thu Mar  7 19:20:48.929 UTC

Proposal Name              : proposal1
================================================================================
Status                     : Complete
--------------------------------------------------------------------------------
Total Number of Enc. Alg.  : 1
   Encr. Alg.              : CBC-AES-256
--------------------------------------------------------------------------------
Total Number of Hash. Alg. : 1
   Hash. Alg.              : SHA 1
--------------------------------------------------------------------------------

Total Number of PRF. Alg.  : 1
   PRF. Alg.               : SHA 256

--------------------------------------------------------------------------------
Total Number of DH Group   : 1
   DH Group                : Group 20
```

protecting-controller

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

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

no protecting-controller [*ODUk*]

Syntax Description

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

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example

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

```
RP/0/RP0:hostname(config)# controller Odu-Group-Mp2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp 1)# protecting-controller ODUC40/0/0/13
```

protection-attributes connection-mode

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

protection-attributes connection mode [**snc-n**]

no protection-attributes connection mode [**snc-n**]

Syntax Description

snc-n	Configures the SNC-N connection-mode which provides non-intrusive monitoring of the original characteristic information. When this mode is selected, protection is provided at the ODUk path (ODUkP) layer or ODUk TCM (ODUkT) sub-layers.

Command Default

SNC-N

Command Modes

Configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example

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

```
RP/0/RP0:hostname(config)# controller Odu-Group-Mp2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-attributes connection-mode snc-n
```

protection-attributes protection-mode

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

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

Syntax Description

revertive	Configures the revertive protection mode. The revertive mode allows you to configure APS to switch to the working path after it becomes functional. This mode requires configuring the *wait-to-restore* option in seconds. This switch occurs after the following conditions are met: • The condition that caused the traffic switch to the protection path is resolved. • The **wait-to-restore** time has expired.
wait-to-restore	Configures the wait-to-restore timer.
Timer	Specify the time in seconds after which the traffic is automatically switched back to the working controller. Valid range: 300 to 720 seconds. Default value: 300 seconds

Command Default

0

Command Modes

Configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example

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

```
RP/0/RP0:hostname(config)# controller Odu-Group-Mp2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp1)# protection-attributes protection-mode revertive
wait-to-restore-time 400
```

protection-attributes protection-type

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

protection-attributes protection-type [**APSbidi**]
no protection-attributes protection-type [**APSbidi**]

Syntax Description

APSbidi	Configures the 1+1 bi-directional protection type. This protection type allows the working path to switch to the protection path for both receipt and transmission of traffic. This switch happens regardless of whether the signal fails in the receiving or transmitting direction.

Command Default

OTM_PROT_TYPE_ONE_PLUS_ONE_APS_BIDI

Command Modes

Configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example

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

```
RP/0/RP0:hostname(config)# controller Odu-Group-Mp2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-attributes protection-type APSbidi
```

protection-attributes timers

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

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

Syntax Description

hold-off-time	(Optional) Configures the hold-off time. Once a signal failure is detected on the working path, APS waits until this timer expires before switching the traffic to the protecting path.

timer	Specify the time in milliseconds. You can configure the timer only in multiples of hundred. Valid range:100 to 10000 milliseconds Default value: 0

Command Default 0

Command Modes Configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example

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

```
RP/0/RP0:hostname(config)# controller Odu-Group-Mp2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-attributes timers hold-off-time 1000
```

protection-switching

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

Note If the protection controller is active, configuring the protection switching to lockout automatically switches the traffic to the working controller.

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

Syntax Description

operate	Configures the protection switching.
lockout	Configures the working path as a locked out resource, forcing the use of working controller and preventing the traffic to be automatically switched to the protection controller.
odu-dest	Configures the controller in which the working path is to be locked out.
ODUk	Specify the name of the controller.

R/S/I/P	Specify the Rack/Slot/Instance/Port of the working path.

Command Default None

Command Modes Configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example

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

```
RP/0/RP0:hostname(config)# controller Odu-Group-Mp2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp 1)# protection-switching operate lockout odu-dest
ODUC4 0/0/0/12
RP/0/RP0:hostname(config-odu-group-mp 1)# commit
```

query url

To specify Lightweight Directory Access Protocol (LDAP) protocol support, use the **query url** command in trustpoint configuration mode. To remove the query URL from the configuration, use the **no** form of this command.

query url *LDAP-URL*
no query url *LDAP-URL*

Syntax Description

LDAP-URL	URL of the LDAP server (for example, ldap://another-server). This URL must be in the form of ldap://server-name where server-name is the host Domain Name System (DNS) name or IP address of the LDAP server.

Command Default The URL provided in NCS 1004 certificate's CRLDistributionPoint extension is used.

Command Modes Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines LDAP is a query protocol used when NCS 1004 retrieves the Certificate Revocation List (CRL). The certification authority (CA) administrator should be able to tell you whether the CA supports LDAP; if the CA supports LDAP, the CA administrator can tell you the LDAP location where certificates and certificate revocation lists should be retrieved.

To change the query URL, repeat the **query url** command to overwrite the previous URL.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows the configuration required to declare a CA when the CA supports LDAP:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)# crypto ca trustpoint myca
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# query url ldap://my-ldap.domain.com
```

router-id ipv4 unicast

To configure the LMP unicast or neighbor router ID for GMPLS, use the **router-id** command in the LMP GMPLS UNI configuration or LMP GMPLS UNI neighbor configuration mode.

router-id ipv4 unicast *address*

Syntax Description

address	Specifies the GMPLS UNI optical router-id (IPv4 address).

Command Default

None

Command Modes

LMP GMPLS UNI configuration

LMP GMPLS UNI neighbor configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to specify a router ID (address 10.10.4.4) for GMPLS UNI.

```
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#router-id ipv4 unicast 10.10.4.4
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)
```

The following example shows how to specify the neighbor router ID 10.10.5.5 for GMPLS UNI.

```
RP/0/RP0/CPU0:ios(config)#lmp
RP/0/RP0/CPU0:ios(config-lmp)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni)#neighbor UN01
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-nbr-UN01)#router-id ipv4 unicast 10.10.5.5
RP/0/RP0/CPU0:ios(config-lmp-gmpls-uni-nbr-UN01)#
```

rsakeypair

To specify a named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint, use the **rsakeypair** command in trustpoint configuration mode. To reset the RSA key pair to the default, use the **no** form of this command.

rsakeypair *keypair-label*
no rsakeypair *keypair-label*

Syntax Description

keypair-label	RSA key pair label that names the RSA key pairs.

Command Default

If the RSA key pair is not specified, the default RSA key is used for this trustpoint.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **rsakeypair** command to specify a named RSA key pair generated using the **crypto key generate rsa** command for this trustpoint.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to specify the named RSA key pair key1 for the trustpoint myca:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)# crypto ca trustpoint myca
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# rsakeypair key1
```

sftp-password (trustpoint)

To secure the FTP password, use the **sftp-password** command in trustpoint configuration mode. To disable this feature, use the **no** form of this command.

sftp-password {*clear text* | **clear** *text* | **password** *encrypted string*}
no sftp-password {*clear text* | **clear** *text* | **password** *encrypted string*}

Syntax Description

clear text	Clear text password and is encrypted only for display purposes.
password *encrypted string*	Enters the password in an encrypted form.

Command Default The *clear text* argument is the default behavior.

Command Modes Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines Passwords are stored in encrypted form and not as plain text. The command-line interface (CLI) contains the provisioning (for example, clear and encrypted) to specify the password input.

The username and password are required as part of the SFTP protocol. If you specify the URL that begins with the prefix (sftp://), you must configure the parameters for the **sftp-password** command under the trustpoint. Otherwise, the certificate from the SFTP server, which is used for manual certificate enrollment, cannot be retrieved.

Task ID

Task ID	Operations
crypto	read, write

Examples The following example shows how to secure the FTP password in an encrypted form:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)# crypto ca trustpoint msiox
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# sftp-password password xxxxxx
```

sftp-username (trustpoint)

To secure the FTP username, use the **sftp-username** command in trustpoint configuration mode. To disable this feature, use the **no** form of this command.

sftp-username *username*
no sftp-username *username*

Syntax Description

username	Name of the user.

Command Default None

Command Modes Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

The **sftp-username** command is used only if the URL has (sftp://) in the prefix. If (sftp://) is not specified in the prefix, the manual certificate enrollment using SFTP fails.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to secure the FTP username:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# configure
RP/0/0RP0RSP0/CPU0:ios:hostname(config)# crypto ca trustpoint msiox
RP/0/0RP0RSP0/CPU0:ios:hostname(config-trustp)# sftp-username tmordeko
```

show configuration commit changes

To display the changes made to the running configuration by previous configuration commits, a configuration commit, or for a range of configuration commits, use the **show configuration commit changes** command in EXEC, administration EXEC, administration configuration, or global configuration mode.

show configuration commit changes { *commit-id* | **since** *commit-id* | **last** *number-of-commits* | **original** *last-modified* | **all** } [**diff**]

Syntax Description

since	Displays all changes committed to the running configuration since (and including) a specific configuration commit.
commit-id	Displays configuration changes for a specific configuration commit.
last *number-of-commits*	Displays the changes made to the running configuration during the last number of configuration commits specified for the *number-of-commits* argument.
original *last-modified*	Displays the original content of the actual commit operation before policy modifications by commit scripts.
all	Displays commit ID and configurations completed for last 100 commits.
diff	(Optional) Displays added lines, changed lines, and deleted lines.

Command Default None

Command Modes EXEC

Administration EXEC

Administration configuration

Global configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines Each time a configuration is committed with the **commit** command, the configuration commit operation is assigned a commit ID. The **show configuration commit changes** command displays the configuration changes made since the specified commit.

To display a list of the available commit IDs, enter the **show configuration commit list** command. You can also display the commit IDs by entering the **show configuration commit changes** command with the online help function (**?**).

You cannot view commit IDs from a different release if the syntax or semantics of the configuration changed in the current release.



Note Syntax of a configuration refers to its structure and format, while the semantics of a configuration refers to its backend interpretation.

The following example shows sample output from the **show configuration commit changes** command with the *commit-id* argument. In this example, the output displays the changes made in the configuration commit assigned commit ID 1000035693.

```
RP/0/RP0/CPU0:ios#show configuration commit changes 1000035693
Tue Feb 28 14:28:03.404 UTC
!! Building configuration...
interface GCC20/1/0/12
 ipv4 address 10.1.1.2 255.255.255.0
!
end
```

The following example shows sample output from the **show configuration commit changes** command with the **since** *commit-id* keyword and argument. In this example, the output displays the configuration changes made since the configuration commit assigned commit ID 1000035693 was committed.

```
RP/0/RP0/CPU0:ios#show configuration commit changes since 1000035693
Tue Feb 28 14:29:42.858 UTC
!! Building configuration...
controller ODUC40/1/0/12
 no gcc2
!
no interface preconfigure GCC20/1/0/12
no keyring keyring_all_in_one
no ikev2 profile profile_all_in_one
```

```
end
```

The following example shows sample output from the **show configuration commit changes** command with the **diff** keyword. In the display, the following symbols signify changes:

+ indicates an added line.

– indicates a deleted line.

# indicates a modified line.

```
RP/0/RP0/CPU0:ios#show configuration commit changes since 1000035681 diff
Tue Feb 28 14:32:24.349 UTC
!! Building configuration...
-  logging console disable
#  line default
#   exec-timeout 0 0
#  !
-  controller ODUC40/1/0/12
-   gcc2
-  !
-  interface preconfigure GCC20/1/0/12
-   ipv4 address 10.1.1.2 255.255.255.0
-  !
-  keyring keyring_all_in_one
-   peer link_1
-    pre-shared-key password 11021C1C46
-    address 10.1.1.2 255.255.255.0
-   !
-  !
end
```

The following example shows sample output from the **show configuration commit changes** command with the **all** keyword. In this example, the output displays the list of configurations that are committed in last 100 commits along with their commit-ID.

```
RP/0/RP0/CPU0:ios#show configuration commit changes all
Tue Feb 28 14:33:33.772 UTC

 Commit ID :  1000035611
-------------------------------------------------------
!! Building configuration...
controller Optics0/3/0/12
 shutdown
!
end


 Commit ID :  1000035612
-------------------------------------------------------
!! Building configuration...
controller Optics0/3/0/12
 no shutdown
!
end


 Commit ID :  1000035613
-------------------------------------------------------
!! Building configuration...
controller Odu-Group-Mp1 signal Otn odu-type ODUC4
 no protection-switching operate lockout odu-dest ODUC40/3/0/12
!
```

```
end
```

show controllers [odu-group-mp]

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

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

Syntax Description

odu-group-mp	Displays details of the ODU group controller pertaining to management plane.
Group ID	Name of the ODU group controller.
protection-detail	Displays the hardware information of the ODU group controller.

Command Modes

Exec mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example 1

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

```
RP/0/RP0/CPU0:ios# show  controllers odu-group-mp 2
```

```
ODU  Group Information
----------------------------------------------------------------
ODU GROUP ID                                        : 2
Controller State                                    : Up

 WORKING CONTROLLER

ODU NAME                                            :  ODUC4 0/0/0/12
ODU ROLE                                            :  WORKING
ODU STATE                                           : Active_tx
Local Failure                                       :  Yes
Remote Failure                                      :  Yes

 PROTECTED CONTROLLER

ODU NAME                                            :  ODUC4 0/0/0/13
ODU ROLE                                            :  PROTECT
ODU STATE                                           : Active
Local Failure                                       :  No
Remote Failure                                      :  No
```

```
PROTECTION PARAMETERS :
Connection Mode                                 : SNC_N
Protection Type                                 : 1+1 Bidirectional Protection
Tcmid                                           : 0
Protection Mode                                 : Revertive
Hold off timer                                  : 1000
Wait-to-restore timer                           : 400000 ms


Detected Alarms                                 :Switched To Protection
```

Example 2

This example shows how to display the harware details of an ODU group controller:

```
RP/0/RP0/CPU0:ios#show  controllers odu-group-mp 2 protection-detail
```

```
Tue Sep 13 12:22:41.316 UTC

ODU  Group Information
---------------------------------------------------------------
LOCAL
                Request State                   : Signal Failed
                Request signal                  : 0
                Bridge signal                   : 1
                Bridge Status                   : 1+1
REMOTE
                Request State                   : Signal Failed
                Request signal                  : 0
                Bridge signal                   : 1
                Bridge Status                   : 1+1
WORKING
                Controller Name                 : ODUC40_0_0_12
                ODU STATE                       : Active_tx
                Local Failure                   : Signal Failure
                Remote Failure                  : Signal Failure
                WTR Left                        : 0 ms

PROTECT
                Controller Name                 : ODUC40_0_0_13
                ODU STATE                       : Active
                Local Failure                   : State Ok
                Remote Failure                  : State Ok
                WTR Left                        : 0 ms

Client
                Controller Name                 : ODUC40_0_0_0
                ODU STATE                       : Not Present


Wait to restore                                 : 400000 ms
Hold-off-timer                                  : 1000 ms
Current State                                   :  Signal failed on Working
Previous State                                  : No Request State
```

show crypto ca certificates

To display information about your certificate and the certification authority (CA) certificate, use the **show crypto ca certificates** command in EXEC mode.

show crypto ca certificates

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Use the **show crypto ca certificates** command to display information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto ca enroll** command).
- CA certificate, if you have received the certificate (see the **crypto ca authenticate** command).

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ca certificates** command:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# show crypto ca certificates
Trustpoint       : msiox
================================================
CAa certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
certificate
  Status         : Available
  Key usage      : Signature
  Serial Number  : 38:6B:C6:B8:00:04:00:00:01:45
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 192.0.2.89
    Serial Number: 8cd96b64
  Issued By      :
```

```
        cn=CA2
  Validity Start : 08:30:03 UTC Mon Apr 10 2006
  Validity End   : 08:40:03 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: MS-IOX
certificate
  Status         : Available
  Key usage      : Encryption
  Serial Number  : 38:6D:2B:A7:00:04:00:00:01:46
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 198.51.100.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:31:34 UTC Mon Apr 10 2006
  Validity End   : 08:41:34 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: msiox
```

The following is a sample output with multi-tier CA. The command output displays the **Trusted Certificate Chain** field if there is one or more subordinate CAs involved in the hierarchy.

```
RP/0/RP0/CPU0:ios#show crypto ca certificates test-ca
Mon Feb  6 09:03:53.019 UTC

Trustpoint       : test-ca
==================================================
CA certificate
  Serial Number  : 10:01
  Subject:
            CN=SUB_CA_CERT,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Issued By      :
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 12:31:40 UTC Sun Jun 14 2020
  Validity End   : 12:31:40 UTC Wed Jun 12 2030

  CRL Distribution Point
            http://10.105.236.78/crl_akshath_two_level_ca/crl.der
  SHA1 Fingerprint:
             D8E0C11ECED96F67FDBC800DB6A126676A76BD62
Trusted Certificate Chain
  Serial Number  : 0F:A0:06:7A:C9:5E:A9:E7:61:A2:B9:2B:27:D1:D6:8F:3D:51:43:3B
  Subject:
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Issued By      :
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 13:12:32 UTC Sun Jun 07 2020
  Validity End   : 13:12:32 UTC Sat Jun 02 2040

  CRL Distribution Point
            http://10.105.236.78/crl_akshath_two_level_ca/crl.der
  SHA1 Fingerprint:
             08E71248FB7578614442E713AC87C461D173952F
certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : 28:E5
  Subject:
            CN=test
  Issued By      :
            CN=SUB_CA_CERT,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
```

```
  Validity Start : 08:49:54 UTC Mon Feb 06 2023
  Validity End   : 08:49:54 UTC Wed Mar 08 2023
  SHA1 Fingerprint:
            6C8644FA67D9CEBC7C5665C35838265F578835AB
Associated Trustpoint: test-ca
```

show crypto key mypubkey ed25519

To display the Ed25519 crypto public keys of NCS 1004, use the **show crypto key mypubkey ed25519** command in in EXEC mode.

show crypto key mypubkey ed25519

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

This example shows the sample output of the **show crypto key mypubkey ed25519** command:

```
RP/0/0RP0RSP0/CPU0:ios# show crypto key mypubkey  ed25519

Mon Nov 30 07:05:06.532 UTC
Key label: the_default
Type : ED25519
Size : 256
Created : 07:03:17 UTC Mon Nov 30 2020
Data :
FF0ED4E7 71531B3D 9ED72C48 3F79EC59 9EFECCC3 46A129B2 FAAA12DD EE9D0351
```

Related Commands

Command	Description
crypto key generate ed25519, on page 36	Generates Ed25519 crypto key pairs.
crypto key zeroize ed25519, on page 39	Deletes all Ed25519 keys from NCS 1004.

show crypto key mypubkey rsa

To display the Rivest, Shamir, and Adelman (RSA) public keys for NCS 1004, use the **show crypto key mypubkey rsa** command in EXEC mode.

show crypto key mypubkey rsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **show crypto key mypubkey rsa** command:

```
RP/0/0RP0RSP0/CPU0:ios:hostname# show crypto key mypubkey rsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF8CDF
5BFCA055 DA4D164D F6EDB78B 926B1DDE 0383027F BA71BCC6 9D5592C4 5BA8670E
35CD19B7 1C973A46 62CC5F8C 82BD596C F292410F 8E83B753 4BA71BAC 41AB6B60
F34A2499 EDE11639 F88B4210 B2A0CF5F DD678C36 0D8B7DE1 A2AB5122 9ED947D5
76CF5BCD D9A2039F D02841B0 7F8BFF97 C080B791 10A9ED41 00FB6F40 95020301
0001

Key label: the_default
Type : RSA General purpose
Size : 512
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C7DE73 7B3EA447
CCE8F3DF DD1327D8 C1C30C45 2EEB4981 B1B48D2B 1AF14665 178058FB 8F6BB6BB
E08C6163 FA0EE356 395C8E5F 2AC59383 0706BDDF EC8E5822 9B020301 0001
```

show linux security audit

To view the details of the Linux security audit information, use the **show linux security audit** command in XR EXEC mode.

show linux security audit

{ **monitor status** { *rule-group* | | **detail** *rule-group* } | | **logging syslog** }

Syntax Description

monitor	Displays the audit monitor information.
status	Displays the audit monitor status.
rule-group	Displays the status of the specified rule group. This field can take these values: **all, authlog-files, cron-files, dns-client-files, docker, file-deletion, file-perm-changes, kernel-module-mgmt, process-audits, system-login-reboot, system-software, system-time-change, user-group-config-files, user-privilege-mgmt, xr-software**
detail	Displays the detailed status of the specified rule group.
logging	Displays the audit logging information.
syslog	Displays the remote syslog server information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

Use the **show linux security audit monitor status** command to verify the general status of all active audit rule groups.

Use the **show linux security audit logging syslog** command to verify whether audit log forwarding is enabled and to view the configured remote syslog server.

Example

This example displays the audit log forwarding details.

```
RP/0/RP0/CPU0:ios# show linux security audit logging syslog
status: enabled
syslog-server(s):
ipaddr: 10.0.1.2 vrf: default port: 514
ipaddr: 2001:db8::1 vrf: default port: 514
```

sak-rekey-interval

To configure the key lifetime for the child security associations (SA), use the **sak-rekey-interval** command in OTNSec policy configuration mode.

sak-rekey-interval *seconds*

Syntax Description

seconds	SAK rekey timer in seconds. The range is from 30 to 1209600 seconds.

Command Default

None

Command Modes

OTNSec policy configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an OTNSec policy is configured.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 11 15:16:58.417 UTC
RP/0/RP0/CPU0:ios(config)#otnsec policy otnsec-policy1
RP/0/RP0/CPU0:ios(config-otnsec-policy)#cipher-suite AES-GCM-256
RP/0/RP0/CPU0:ios(config-otnsec-policy)#security-policy must-secure
RP/0/RP0/CPU0:ios(config-otnsec-policy)#sak-rekey-interval 120
RP/0/RP0/CPU0:ios(config-otnsec-policy)#commit
```

The following is a sample of an OTNSec policy.

```
RP/0/RP0/CPU0:ios#show run otnsec policy otnsec-policy1
Tue Mar 12 11:14:03.591 UTC
otnsec policy otnsec-policy1
 cipher-suite AES-GCM-256
 security-policy must-secure
 sak-rekey-interval 120
!
```

security-policy

To specify the security for OTNSec policy, use the **security-policy** command in OTNSec policy configuration mode.

security-policy **must-secure**

Syntax Description

must-secure	Mandatory security for OTNSec.

Command Default None

Command Modes OTNSec policy configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which an OTNSec policy is configured.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 11 15:16:58.417 UTC
RP/0/RP0/CPU0:ios(config)#otnsec policy otnsec-policy1
RP/0/RP0/CPU0:ios(config-otnsec-policy)#cipher-suite AES-GCM-256
RP/0/RP0/CPU0:ios(config-otnsec-policy)#security-policy must-secure
RP/0/RP0/CPU0:ios(config-otnsec-policy)#sak-rekey-interval 120
RP/0/RP0/CPU0:ios(config-otnsec-policy)#commit
```

The following is a sample of an OTNSec policy.

```
RP/0/RP0/CPU0:ios#show run otnsec policy otnsec-policy1
Tue Mar 12 11:14:03.591 UTC
otnsec policy otnsec-policy1
 cipher-suite AES-GCM-256
 security-policy must-secure
 sak-rekey-interval 120
!
```

session-id

To configure the session ID for OTNSec on ODU4 controller, use the **session-id** command in OTNSec configuration mode.

session-id *session-id*

Syntax Description

session-id	Session ID. The range is from 1 to 65535.

Command Default None

Command Modes OTNSec configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following is a sample in which OTNSec is configured on ODU4 controllers.

```
RP/0/RP0/CPU0:ios#configure
Mon Mar 12 12:10:21.374 UTC
RP/0/RP0/CPU0:ios(config)#controller ODU4 0/1/0/0/1
RP/0/RP0/CPU0:ios(config-odu4)#otnsec
RP/0/RP0/CPU0:ios(config-otnsec)#source ipv4 10.0.0.1
RP/0/RP0/CPU0:ios(config-otnsec)#destination ipv4 10.0.0.2
RP/0/RP0/CPU0:ios(config-otnsec)#session-id 9000
RP/0/RP0/CPU0:ios(config-otnsec)#policy otnsec-policy1
RP/0/RP0/CPU0:ios(config-otnsec)#ikev2 profile profile1
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#commit
Mon Mar 12 12:14:17.609 UTC
RP/0/RP0/CPU0:ios(config-ikev2-profile-profile1)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

The following is a running configuration on an ODU4 controller.

```
RP/0/RP0/CPU0:ios#show run controller ODU4 0/1/0/0/1
Tue Mar 12 12:20:49.153 UTC
controller ODU40/1/0/0/1
 gcc2
 otnsec
  policy otnsec-policy1
  source ipv4 10.0.0.1
  destination ipv4 10.0.0.2
  session-id 9000
 !
!
```

show alarms

To display alarms in brief or detail, use the **show alarms** command in XR EXEC mode or Administration EXEC mode.

show alarms brief [card [location *location* **] | rack | system] [active | history]]**

show alarms detail [card [location *location* **]| rack | system] [active | clients | history | stats]]**

Syntax Description

brief		Displays alarms in brief.
card		Displays card scope alarms related data.
rack		Displays rack scope alarms related data.
system		Displays system scope alarms related data.
location	*location*	Specifies the target location in the *rack/slot* notation.
active		Displays active alarms.
history		Displays alarm history.
detail		Displays alarms in detail.

clients	Displays clients associated with the service.
stats	Displays service statistics.

Command Default

None

Command Modes

XR EXEC

Administration EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

This command displays the alarms in brief or detail. The command displays only the administration alarms in admin EXEC mode and all the alarms in XR EXEC mode.

Example

The following example shows the output of the **show alarms** command.

sysadmin-vm:0_RP0# **show alarms**

```
Wed Mar  20 05:25:53.146 UTC+00:00

-------------------------------------------------------------------------------------------------
Active Alarms
-------------------------------------------------------------------------------------------------
Location          Severity      Group           Set time            Description
-------------------------------------------------------------------------------------------------
0/PM0             major         environ         03/19/19 21:37:29   Power Module Output
Disabled
0                 major         environ         03/19/19 21:37:35   Power Module redundancy
 lost.
```

RP/0/RP0/CPU0:ios# **show alarms brief card location 0/RP0/CPU0 active**

```
Wed Mar 20 05:26:52.116 UTC

-------------------------------------------------------------------------------------------------
Active Alarms
-------------------------------------------------------------------------------------------------
Location        Severity     Group            Set Time                    Description

-------------------------------------------------------------------------------------------------
0/PM0           Major        FPD_Infra        03/19/2019 21:39:04 UTC    One Or More FPDs
Need Upgrade
                                                                         Or Not In Current
 State
```

show controllers

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

show controllers *controllertype R/S/I/P* [**pm** { **current** | **history** } { **30 sec** | **15-min** | **24-hour** } { **optics** | **ether** | **pcs** | **prbs** | **stm** | **ocn** } *linenumber* { **otn** | **fec** }] [**fastpoll**]

To view the the bits-per-symbol or baud rate of the optics controller for a specific range use the following command:

show controllers optics *R/S/I/P* { **bps-range** *bps-range* | **baud-rate-range** *baud-range* } **| include** *data-rate* **| include** *fec-type*

Syntax Description

controllertype	Type of the controller. The possible values are HundredGigECtrlr, CoherentDSP, ODU4, ODUC4, oc192, stm64, and Optics.
R/S/I/P	Rack/Slot/Instance/Port of the controller.
pm	Displays performance monitoring parameters for the controller.
current	Displays the current performance monitoring data in 30 second, 15 minute, and 24-hour intervals.
history	Displays the historical performance monitoring data in 30 second, 15 minute, and 24-hour intervals.
optics | **ether** | **pcs** | **prbs** | **stm** | **ocn**	optics to display the PM data for Optics controller, ether, pcs, and prbs to display the PM data for Ethernet controller. stm and ocn for STM64 and OC192 controllers.
linenumber	Line number to display performance monitoring data. The range is 1–4.
otn | **fec**	Displays OTN PM data or FEC PM data for CoherentDSP controller.
bps-range *bps-range*	Displays the BPS for the specified range.
baud-rate-range *baud-range*	Displays the baud rates for the specified range.
| include	Filters the show command output so that it displays only lines that contain a particular regular expression.
data-rates	Data rate for which the BPS or baud rate is displayed.
fec-type	FEC type for which the BPS or baud rate is displayed.
fastpoll	The fastpoll data is displayed.

Usage Guidelines

The following table describes the PRBS parameters.

Parameter	Description
EBC	Cumulative count of PRBS bit errors in the sampling window (15 min or 24 hour). Bit errors are accumulated only if PRBS signal is locked.
FOUND-COUNT	Number of state transitions from signal unlocked state to locked state in the sampling window. If no state change is observed in the interval, the count will be zero.
LOST-COUNT	Number of state transitions from signal locked state to signal unlocked state in the sampling window. If there is no state change observed in the interval, the count is zero.
FOUND-AT-TS	Latest timestamp when the PRBS state switches from unlocked state to locked state in the sampling window. If no state change is observed in the sampling window, this value is null.
LOST-AT-TS	Latest timestamp when the PRBS state switches from locked state to unlocked state in the sampling window. If no state change is observed in the sampling window, this value is null.
CONFIG-PTRN	Configured PRBS pattern on the port.

- Total TX Power and Total RX Power: For multi-lane controller optics, total power is calculated by converting each lane power value from dBm to mW, and adding each lane power. Total power in mW must then be converted to dBm.

  Total power in mW = [(Lane 1 power in mW) + (Lane 2 power in mW) + (Lane 3 power in mW) + (Lane 4 power in mW)]

  Total power in dBm = Converted value of total power in mW to dBm

Command Default

The status and configuration information of all the interfaces is displayed.

Command Modes

XR EXEC

Command History

Release	Modification
7.0.1	This command was introduced.
7.1.1	**pcs** keyword was added.
7.3.1	The keyword **fastpoll** was added.
7.8.1	The **ODUC4** *controllertype* argument was added.
7.10.1	**oc192 and stm64,** *controllertype* arguments were added.

Examples

The following is a sample to view the laser squelch status on the Ethernet controller.

RP/0/RP0/CPU0:ios#**show controller HundredGigECtrlr 0/1/0/10**

```
RP/0/RP0/CPU0:ios#show controller HundredGigECtrlr 0/1/0/10
Fri Feb 22 15:18:47.011 UTC
Operational data for interface HundredGigECtrlr0/1/0/10:

State:
    Administrative state: enabled
    Operational state: Up
    LED state: Green On
    Maintenance: Disabled
    AINS Soak: None
      Total Duration: 0 hour(s) 0 minute(s)
      Remaining Duration: 0 hour(s) 0 minute(s) 0 second(s)
    Laser Squelch: Enabled

Phy:
    Media type: Not known
    Statistics:
        FEC:
            Corrected Codeword Count: 0
            Uncorrected Codeword Count: 0

Autonegotiation disabled.

Operational values:
    Speed: 100Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    BER monitoring:
        Not supported
    Forward error correction: Standard (Reed-Solomon)
    Holdoff Time: 0ms
```

The following is a sample to view the hold off timer configured on the ethernet controller.

RP/0/RP0/CPU0:ios#**show controller HundredGigECtrlr 0/1/0/10**

```
Fri Feb 22 18:58:06.888 UTC
Operational data for interface HundredGigECtrlr0/1/0/10:

State:
    Administrative state: enabled
    Operational state: Up
    LED state: Green On
    Maintenance: Disabled
    AINS Soak: None
      Total Duration: 0 hour(s) 0 minute(s)
      Remaining Duration: 0 hour(s) 0 minute(s) 0 second(s)
    Laser Squelch: Enabled

Phy:
    Media type: Not known
    Statistics:
        FEC:
            Corrected Codeword Count: 0
            Uncorrected Codeword Count: 0

Autonegotiation disabled.

Operational values:
    Speed: 100Gbps
```

```
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    BER monitoring:
        Not supported
    Forward error correction: Standard (Reed-Solomon)
    Holdoff Time: 3000ms
```

The following is a sample to view the loopback configured on the ethernet controller.

RP/0/RP0/CPU0:ios#**show controller HundredGigECtrlr 0/1/0/10**

```
Fri Feb 22 20:01:00.521 UTC
Operational data for interface HundredGigECtrlr0/1/0/10:

State:
    Administrative state: enabled
    Operational state: Up
    LED state: Green On
    Maintenance: Enabled
    AINS Soak: Pending
      Total Duration: 0 hour(s) 30 minute(s)
      Remaining Duration: 0 hour(s) 30 minute(s) 0 second(s)
    Laser Squelch: Enabled

Phy:
    Media type: Not known
    Statistics:
        FEC:
            Corrected Codeword Count: 0
            Uncorrected Codeword Count: 6

Autonegotiation disabled.

Operational values:
    Speed: 100Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: Line
    BER monitoring:
        Not supported
    Forward error correction: Standard (Reed-Solomon)
    Holdoff Time: 0ms
```

The following example displays the optics controller statistics with AINS Soak in running state.

RP/0/RP0/CPU0:ios#**show controller optics 0/1/0/3**

```
Thu Feb 21 19:45:41.088 UTC

 Controller State: Up

 Transport Admin State: Automatic In Service

 Laser State: On

 LED State: Green

 Optics Status

         Optics Type:  Grey optics

         Alarm Status:
```

```
        -------------
        Detected Alarms: None


        LOS/LOL/Fault Status:

        Alarm Statistics:

        -------------
        HIGH-RX-PWR = 0            LOW-RX-PWR = 0
        HIGH-TX-PWR = 0            LOW-TX-PWR = 0
        HIGH-LBC = 0               HIGH-DGD = 0
        OOR-CD = 0                 OSNR = 0
        WVL-OOL = 0                MEA  = 0
        IMPROPER-REM = 0
        TX-POWER-PROV-MISMATCH = 0

        Performance Monitoring: Enable

        THRESHOLD VALUES
        ----------------

        Parameter                 High Alarm  Low Alarm  High Warning  Low Warning
        ------------------------  ----------  ---------  ------------  -----------
        Rx Power Threshold(dBm)          4.9      -12.0           0.0          0.0
        Tx Power Threshold(dBm)          3.5      -10.1           0.0          0.0
        LBC Threshold(mA)                N/A        N/A          0.00         0.00

        LBC High Threshold = 98 %
        Polarization parameters not supported by optics

       Total TX Power = 6.39 dBm

       Total RX Power = 5.85 dBm

        Lane  Laser Bias    TX Power    RX Power  Output Frequency
        ----  ----------  ----------  ----------  ----------------
          1      75.0 %    0.59 dBm    0.63 dBm  230.43 THz
          2      68.6 %    0.06 dBm   -0.68 dBm  230.43 THz
          3      69.0 %    0.26 dBm   -0.63 dBm  230.43 THz
          4      69.1 %    0.56 dBm   -0.10 dBm  230.43 THz

Transceiver Vendor Details

        Form Factor            : QSFP28
        Name                   : CISCO-FINISAR
        Part Number            : FTLC1152RGPL-C2
        Rev Number             : CISCO-FINISAR
        Serial Number          : FNS22150LEC
        PID                    : QSFP-100G-CWDM4-S
        VID                    : V02
        CISCO-FINISAR
        Date Code(yy/mm/dd)    : 18/04/11
        Fiber Connector Type: LC
        Sonet Application Code: Not Set
        Ethernet Compliance Code: 100GBASE-CWDM4

Transceiver Temperature : 32 Celsius


AINS Soak               : Running
AINS Timer              : 0h, 15m
AINS remaining time     : 771 seconds
```

The following is a sample to view the current performance monitoring parameters of the optics controller in 15-minute intervals.

RP/0/RP0/CPU0:ios#**show controller optics 0/1/0/3 pm current 15-min optics 3**

```
Sat Feb  9 19:33:42.480 UTC

Optics in the current interval [19:30:00 - 19:33:42 Sat Feb 9 2019]

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[% ]      : 0.0       0.0       0.0      0.0               NA              NO   100.0
          NA              NO

OPT[dBm]     : -40.00    -40.00    -40.00   -30.00            NA              NO   63.32
          NA              NO

OPR[dBm]     : -40.00    -40.00    -40.00   -30.00            NA              NO   63.32
          NA              NO

FREQ_OFF[Mhz]: 0         0         0        0                 NA              NO   0
          NA              NO
```

The following is a sample to view the current performance monitoring parameters of the Coherent DSP controller in 15-minute intervals.

RP/0/RP0/CPU0:ios#**show controller coherentDSP 0/2/0/1 pm current 15-min fec**

```
Sat Feb  9 11:23:42.196 UTC

g709 FEC in the current interval [11:15:00 - 11:23:42 Sat Feb 9 2019]

FEC current bucket type : Valid
    EC-BITS   : 291612035786            Threshold : 903330                TCA(enable)  :
YES
    UC-WORDS  : 0                       Threshold : 5                     TCA(enable)  :
YES

                MIN       AVG        MAX    Threshold   TCA     Threshold   TCA
                                              (min)    (enable)   (max)    (enable)
PreFEC BER  : 7.1E-03   7.2E-03   8.1E-03     0E-15        NO     0E-15       NO
PostFEC BER :   0E-15     0E-15     0E-15     0E-15        NO     0E-15       NO
```

The following is a sample of an encryption configuration on an ODU4 controller.

RP/0/RP0/CPU0:ios#**show controllers ODU4 0/1/0/0/1 otnsec**

```
Tue Mar 12 17:34:50.660 UTC
Controller Name          : ODU4 0/1/0/0/1
Source ip                : 10.0.0.1
Destination ip           : 10.0.0.2
Session id               : 9000
IKEv2 profile            : Not Configured
Session State            : SECURED

Otnsec policy name       : otnsec-policy1
  cipher-suite           : AES-GCM-256
  security-policy        : Must Secure
```

```
  sak-rekey-interval     : 120
Time to rekey            : 0

Programming Status       :
  Inbound SA(Rx)         :
    AN[0]                :
        SPI              : None
  Outbound SA(Tx)        :
    AN[0]                :
        SPI              : None
```

The following is a sample to view the summary of all the ODU4 controllers.

RP/0/RP0/CPU0:ios#**show controller ODU4 * otnsec summary**

```
Tue Mar 12 15:18:26.299 IST
Controller Name     Source ip           Destination ip      Session id          Session
State
-----------------------------------------------------------------------------------------------
ODU4 0/0/0/0/1      10.1.1.1             10.1.1.2            1                    SECURED
ODU4 0/0/0/0/2      10.1.1.1             10.1.1.2            2                    SECURED
ODU4 0/0/0/0/3      10.1.1.1             10.1.1.2            3                    SECURED
ODU4 0/0/0/0/4      10.1.1.1             10.1.1.2            4                    SECURED
ODU4 0/0/0/0/5      10.1.1.1             10.1.1.2            5                    SECURED
ODU4 0/0/0/1/1      10.1.2.1             10.1.2.2            6                    SECURED
ODU4 0/0/0/1/2      10.1.2.1             10.1.2.2            7                    SECURED
ODU4 0/0/0/1/3      10.1.2.1             10.1.2.2            8                    SECURED
ODU4 0/0/0/1/4      10.1.2.1             10.1.2.2            9                    SECURED
ODU4 0/0/0/1/5      10.1.2.1             10.1.2.2            10                   SECURED
ODU4 0/1/0/0/1      10.1.3.1             10.1.3.2            11                   SECURED
ODU4 0/1/0/0/2      10.1.3.1             10.1.3.2            12                   SECURED
ODU4 0/1/0/0/3      10.1.3.1             10.1.3.2            13                   SECURED
ODU4 0/1/0/0/4      10.1.3.1             10.1.3.2            14                   SECURED
ODU4 0/1/0/0/5      10.1.3.1             10.1.3.2            15                   SECURED
ODU4 0/1/0/1/1      10.1.4.1             10.1.4.2            16                   SECURED
ODU4 0/1/0/1/2      10.1.4.1             10.1.4.2            17                   SECURED
ODU4 0/1/0/1/3      10.1.4.1             10.1.4.2            18                   SECURED
ODU4 0/1/0/1/4      10.1.4.1             10.1.4.2            19                   SECURED
ODU4 0/1/0/1/5      10.1.4.1             10.1.4.2            20                   SECURED
ODU4 0/2/0/0/1      10.1.5.1             10.1.5.2            21                   SECURED
ODU4 0/2/0/0/2      10.1.5.1             10.1.5.2            22                   SECURED
ODU4 0/2/0/0/3      10.1.5.1             10.1.5.2            23                   SECURED
ODU4 0/2/0/0/4      10.1.5.1             10.1.5.2            24                   SECURED
ODU4 0/2/0/0/5      10.1.5.1             10.1.5.2            25                   SECURED
ODU4 0/2/0/1/1      10.1.6.1             10.1.6.2            26                   SECURED
ODU4 0/2/0/1/2      10.1.6.1             10.1.6.2            27                   SECURED
ODU4 0/2/0/1/3      10.1.6.1             10.1.6.2            28                   SECURED
ODU4 0/2/0/1/4      10.1.6.1             10.1.6.2            29                   SECURED
ODU4 0/2/0/1/5      10.1.6.1             10.1.6.2            30                   SECURED
ODU4 0/3/0/0/1      10.1.7.1             10.1.7.2            31                   SECURED
ODU4 0/3/0/0/2      10.1.7.1             10.1.7.2            32                   SECURED
ODU4 0/3/0/0/3      10.1.7.1             10.1.7.2            33                   SECURED
ODU4 0/3/0/0/4      10.1.7.1             10.1.7.2            34                   SECURED
ODU4 0/3/0/0/5      10.1.7.1             10.1.7.2            35                   SECURED
ODU4 0/3/0/1/1      10.1.8.1             10.1.8.2            36                   SECURED
ODU4 0/3/0/1/2      10.1.8.1             10.1.8.2            37                   SECURED
ODU4 0/3/0/1/3      10.1.8.1             10.1.8.2            38                   SECURED
ODU4 0/3/0/1/4      10.1.8.1             10.1.8.2            39                   SECURED
ODU4 0/3/0/1/5      10.1.8.1             10.1.8.2            40                   SECURED
```

The following is a sample to view the PM statistics for encryption.

RP/0/RP0/CPU0:ios#**show controllers ODU4 0/1/0/0/1 pm current 30-sec otnsec**

```
Tue Mar 12 15:19:33.371 IST

OTNSec in the current interval [15:19:30 - 15:19:33 Tue Mar 12 2019]
OTNSEC current bucket type : Valid
InBlocks               : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksEnc            : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksUnEncrypted    : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksProtected      : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksUnProtected    : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksSequenceErrors : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksReplayErrors   : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksAuthErrors     : 0                    Threshold : 0                    TCA(enable)
 :  No
InBlocksZeroed         : 0                    Threshold : 0                    TCA(enable)
 :  No
OutBlocks              : 3425548              Threshold : 0                    TCA(enable)
 :  No
OutBlocksEnc           : 3425548              Threshold : 0                    TCA(enable)
 :  No
OutBlocksUnEncrypted   : 0                    Threshold : 0                    TCA(enable)
 :  No
OutBlocksSequenceErrors: 0                    Threshold : 0                    TCA(enable)
 :  No
OutBlocksZeroed        : 0                    Threshold : 0                    TCA(enable)
 :  No
Last clearing of "show controllers ODU" counters never
```

The following is a sample to view the current performance monitoring parameters for the ethernet controller in 30-second intervals.

RP/0/RP0/CPU0:ios#**show controllers hundredGigECtrlr 0/0/0/2 pm current 30-sec pcs**

```
Tue Nov 19 09:17:26.684 UTC

Ethernet PCS in the current interval [09:17:00 - 09:17:26 Tue Nov 19 2019]

Ethernet PCS current bucket type : Valid
BIP[00] : 0 Threshold : 0 TCA(enable) : NO
BIP[01] : 0 Threshold : 0 TCA(enable) : NO
BIP[02] : 0 Threshold : 0 TCA(enable) : NO
BIP[03] : 0 Threshold : 0 TCA(enable) : NO
BIP[04] : 0 Threshold : 0 TCA(enable) : NO
BIP[05] : 0 Threshold : 0 TCA(enable) : NO
BIP[06] : 0 Threshold : 0 TCA(enable) : NO
BIP[07] : 0 Threshold : 0 TCA(enable) : NO
BIP[08] : 0 Threshold : 0 TCA(enable) : NO
BIP[09] : 0 Threshold : 0 TCA(enable) : NO
BIP[10] : 0 Threshold : 0 TCA(enable) : NO
BIP[11] : 0 Threshold : 0 TCA(enable) : NO
BIP[12] : 0 Threshold : 0 TCA(enable) : NO
BIP[13] : 0 Threshold : 0 TCA(enable) : NO
BIP[14] : 0 Threshold : 0 TCA(enable) : NO
BIP[15] : 0 Threshold : 0 TCA(enable) : NO
BIP[16] : 0 Threshold : 0 TCA(enable) : NO
BIP[17] : 0 Threshold : 0 TCA(enable) : NO
BIP[18] : 0 Threshold : 0 TCA(enable) : NO
BIP[19] : 0 Threshold : 0 TCA(enable) : NO
```

```
FRM-ERR[00] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[01] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[02] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[03] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[04] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[05] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[06] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[07] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[08] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[09] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[10] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[11] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[12] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[13] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[14] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[15] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[16] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[17] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[18] : 0 Threshold : 0 TCA(enable) : NO
FRM-ERR[19] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[00] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[01] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[02] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[03] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[04] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[05] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[06] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[07] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[08] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[09] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[10] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[11] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[12] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[13] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[14] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[15] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[16] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[17] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[18] : 0 Threshold : 0 TCA(enable) : NO
BAD-SH[19] : 0 Threshold : 0 TCA(enable) : NO
ES : 0 Threshold : 0 TCA(enable) : NO
SES : 0 Threshold : 0 TCA(enable) : NO
UAS : 0 Threshold : 0 TCA(enable) : NO
ES-FE : 0 Threshold : 0 TCA(enable) : NO
SES-FE : 0 Threshold : 0 TCA(enable) : NO
UAS-FE : 0 Threshold : 0 TCA(enable) : NO

Last clearing of "show controllers ETHERNET " counters never
RP/0/RP0/CPU0:ios#
```

The following is a sample to view the historical performance monitoring parameters for Ethernet controller in 30-second intervals.

RP/0/RP0/CPU0:ios#**show controllers hundredGigECtrlr 0/0/0/2 pm history 30-sec pcs 1**

```
Tue Nov 19 09:27:49.169 UTC

Ethernet PCS in the current interval [09:27:00 - 09:27:30 Tue Nov 19 2019]

Ethernet PCS current bucket type : Valid
BIP[00] : 0
BIP[01] : 0
BIP[02] : 0
BIP[03] : 0
BIP[04] : 0
```

```
BIP[05] : 0
BIP[06] : 0
BIP[07] : 0
BIP[08] : 0
BIP[09] : 0
BIP[10] : 0
BIP[11] : 0
BIP[12] : 0
BIP[13] : 0
BIP[14] : 0
BIP[15] : 0
BIP[16] : 0
BIP[17] : 0
BIP[18] : 0
BIP[19] : 0
FRM-ERR[00] : 0
FRM-ERR[01] : 0
FRM-ERR[02] : 0
FRM-ERR[03] : 0
FRM-ERR[04] : 0
FRM-ERR[05] : 0
FRM-ERR[06] : 0
FRM-ERR[07] : 0
FRM-ERR[08] : 0
FRM-ERR[09] : 0
FRM-ERR[10] : 0
FRM-ERR[11] : 0
FRM-ERR[12] : 0
FRM-ERR[13] : 0
FRM-ERR[14] : 0
FRM-ERR[15] : 0
FRM-ERR[16] : 0
FRM-ERR[17] : 0
FRM-ERR[18] : 0
FRM-ERR[19] : 0
BAD-SH[00] : 0
BAD-SH[01] : 0
BAD-SH[02] : 0
BAD-SH[03] : 0
BAD-SH[04] : 0
BAD-SH[05] : 0
BAD-SH[06] : 0
BAD-SH[07] : 0
BAD-SH[08] : 0
BAD-SH[09] : 0
BAD-SH[10] : 0
BAD-SH[11] : 0
BAD-SH[12] : 0
BAD-SH[13] : 0
BAD-SH[14] : 0
BAD-SH[15] : 0
BAD-SH[16] : 0
BAD-SH[17] : 0
BAD-SH[18] : 0
BAD-SH[19] : 0
ES : 0
SES : 0
UAS : 0
ES-FE : 0
SES-FE : 0
UAS-FE : 0

Last clearing of "show controllers ETHERNET " counters never
RP/0/RP0/CPU0:ios#
```

The following is a sample to view the Pseudo Random Binary Sequence (PRBS) performance monitoring parameters on the coherentDSP controller.

RP/0/RP0/CPU0:ios#**show controllers coherentDSP 0/0/0/1 pm current 15-min prbs**

```
Mon Feb 13 00:58:48.327 UTC
PRBS in the current interval [00:45:00 - 00:58:48 Mon Feb 13 2019]
PRBS current bucket type : Valid
EBC : 40437528165
FOUND-COUNT : 1 FOUND-AT-TS : 00:51:22 Mon Feb 13 2019
LOST-COUNT : 1 LOST-AT-TS : 00:52:52 Mon Feb 13 2019
CONFIG-PTRN : PRBS_PATTERN_PN31
Last clearing of "show controllers OTU" counters never
```

The following is a sample to view the fastpoll data using the show controller optics fastpoll command:

```
RP/0/RP0/CPU0:G_BLR#sh controllers optics 0/0/0/0 fastpoll
Thu Mar  4 07:36:06.479 UTC

Index   Timestamp           Interval   SOP Param1             SOP Param2             SOP
Param3
                            (in msec)
--------------------------------------------------------------------------------------------------
323997   1614843319774376    71        0.75634020566940308    0.65416425466537476
0.00256355479359627
323997   1614843319842376    68        0.73894464969635010    0.67360454797744751
-0.01290932949632406
323997   1614843319911376    69        0.74565875530242920    0.66615802049636841
0.01333658862859011
323997   1614843319979376    68        0.75981932878494263    0.64986115694046021
-0.01788384653627872
323997   1614843320034376    55        0.75841546058654785    0.65172278881072998
-0.00027466658502817
323997   1614843320091376    57        0.75084686279296875    0.66032898426055908
-0.01101718191057444
323997   1614843320146376    55        0.74700152873992920    0.66475415229797363
-0.00756859034299850
323997   1614843320201376    55        0.74233222007751465    0.66988128423690796
0.01202429272234440
323997   1614843320259376    58        0.75130468606948853    0.65990173816680908
0.00363170262426138
323997   1614843320316376    57        0.75209814310073853    0.65892511606216431
-0.01126132998615503
323997   1614843320372376    56        0.74962615966796875    0.66182440519332886
0.00259407330304384
323997   1614843320427376    55        0.75087738037109375    0.66035950183868408
-0.00869777519255877
323997   1614843320483376    56        0.75930052995681763    0.65068513154983521
-0.00244148075580597
```

The following is a sample to view the 8QAM modulation on the 200G muxponder mode for the OTN-XP card.

```
RP/0/RP0/CPU0:ios#show controllers optics 0/1/0/12
Wed Jun  2 17:17:29.652 UTC
 Controller State: Up
 Transport Admin State: In Service
 Laser State: On
 LED State: Green
 Optics Status

         Optics Type:  <Unknown> DWDM
         DWDM carrier Info: C BAND, MSA ITU Channel=61, Frequency=193.10THz,
         Wavelength=1552.524nm
```

```
        Alarm Status:
        -------------
        Detected Alarms: None


        LOS/LOL/Fault Status:

        Alarm Statistics:

        -------------
        HIGH-RX-PWR = 0            LOW-RX-PWR = 1
        HIGH-TX-PWR = 0            LOW-TX-PWR = 1
        HIGH-LBC = 0               HIGH-DGD = 0
        OOR-CD = 0                 OSNR = 1
        WVL-OOL = 0                MEA  = 0
        IMPROPER-REM = 0
        TX-POWER-PROV-MISMATCH = 0
        Laser Bias Current = 0.0 %
        Actual TX Power = 0.97 dBm
        RX Power = 1.47 dBm
        RX Signal Power = 17.67 dBm
        Frequency Offset = 82 MHz

        Performance Monitoring: Enable

        THRESHOLD VALUES
        ----------------

        Parameter                High Alarm  Low Alarm  High Warning  Low Warning
        -----------------------  ----------  ---------  ------------  -----------
        Rx Power Threshold(dBm)          3.0      -31.5           0.0          0.0
        Tx Power Threshold(dBm)          3.0      -12.0           0.0          0.0
        LBC Threshold(mA)                N/A        N/A          0.00         0.00

        LBC High Threshold = 90 %
        Configured Tx Power = 1.00 dBm
        Configured CD High Threshold = 96000 ps/nm
        Configured CD lower Threshold = -96000 ps/nm
        Configured OSNR lower Threshold = 13.70 dB
        Configured DGD Higher Threshold = 67.00 ps
        Baud Rate =  42.2082633972 GBd
        Bits per Symbol = 3.0000000000  bits/symbol
        Modulation Type: 8QAM
        Chromatic Dispersion 2 ps/nm
        Configured CD-MIN -48000 ps/nm  CD-MAX 48000 ps/nm
        Polarization Mode Dispersion = 0.0 ps
        Second Order Polarization Mode Dispersion = 72.00 ps^2
        Optical Signal to Noise Ratio = 34.10 dB
        SNR = 18.40 dB
        Polarization Dependent Loss = 1.20 dB
        Polarization Change Rate = 0.00 rad/s
        Differential Group Delay = 2.00 ps

Transceiver Vendor Details

        Form Factor            : Not set
        Fiber Connector Type: Not Set
        Otn Application Code: Not Set
        Sonet Application Code: Not Set
        Ethernet Compliance Code: Not set

Transceiver Temperature : 46 Celsius
```

```
 AINS Soak                : None
 AINS Timer               : 0h, 0m
 AINS remaining time      : 0 seconds
```

The following sample verifies the alarm correlation on the inverse muxponder configuration on the OTN-XP card. When trunk port 12 is shut down, LOS alarm is raised and the trunk port 13 also goes down.

```
RP/0/RP0/CPU0:ios#show controllers coherentDSP 0/2/0/12
Thu Sep 30 14:12:54.604 UTC

Port                                        : CoherentDSP 0/2/0/12
Controller State                            : Down
Inherited Secondary State                   : Normal
Configured Secondary State                  : Normal
Derived State                               : In Service
Loopback mode                               : None
BER Thresholds                              : SF = 1.0E-5  SD = 1.0E-7
Performance Monitoring                      : Enable
Bandwidth                                   : 200.0Gb/s

Alarm Information:
LOS = 2 LOF = 0 LOM = 0
OOF = 1 OOM = 0 AIS = 1
IAE = 0 BIAE = 0        SF_BER = 0
SD_BER = 0      BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0     FLEXO_GIDM = 0
FLEXO-MM = 0    FLEXO-LOM = 0   FLEXO-RDI = 1
FLEXO-LOF = 0
Detected Alarms                             : LOS

Bit Error Rate Information
PREFEC  BER                                 : 0.00E+00
POSTFEC BER                                 : 0.00E+00
Q-Factor                                    : 0.00 dB

Q-Margin                                    : 0.00dB

TTI :
        Remote IP addr                      : 0.0.0.0

FEC mode                                    : O_FEC

Flexo-Mode                                  : Enable
Flexo Details:
        Tx GID                              : 1
        TX IID                              : 1, 2,
        Rx GID                              : 0
        RX IID                              : 0, 0,

Flexo Peers Information:
        Controller                          : CoherentDSP0_2_0_13
        OTUCn rate                          : OTUC2


AINS Soak                                   : None
AINS Timer                                  : 0h, 0m
AINS remaining time                         : 0 seconds


RP/0/RP0/CPU0:ios#show controllers coherentDSP 0/2/0/13
```

```
Thu Sep 30 14:12:59.330 UTC

Port                                          : CoherentDSP 0/2/0/13
Controller State                              : Down
Inherited Secondary State                     : Normal
Configured Secondary State                    : Normal
Derived State                                 : In Service
Loopback mode                                 : None
BER Thresholds                                : SF = 1.0E-5  SD = 1.0E-7
Performance Monitoring                        : Enable
Bandwidth                                     : 200.0Gb/s

Alarm Information:
LOS = 1 LOF = 0 LOM = 0
OOF = 0 OOM = 0 AIS = 0
IAE = 0 BIAE = 0        SF_BER = 0
SD_BER = 0      BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0     FLEXO_GIDM = 0
FLEXO-MM = 0    FLEXO-LOM = 0   FLEXO-RDI = 1
FLEXO-LOF = 0
Detected Alarms                               : None

Bit Error Rate Information
PREFEC  BER                                   : 0.00E+00
POSTFEC BER                                   : 0.00E+00
Q-Factor                                      : 15.80 dB

Q-Margin                                      : 9.50dB

TTI :
        Remote IP addr                        : 0.0.0.0

FEC mode                                      : O_FEC

Flexo-Mode                                    : Enable
Flexo Details:
        Tx GID                                : 1
        TX IID                                : 3, 4,
        Rx GID                                : 1
        RX IID                                : 3, 4,

Flexo Peers Information:
        Controller                            : CoherentDSP0_2_0_12
        OTUCn rate                            : OTUC2


AINS Soak                                     : None
AINS Timer                                    : 0h, 0m
AINS remaining time                           : 0 seconds
```

The following sample verifies the loopback on the inverse muxponder configuration on the OTN-XP card:

```
RP/0/RP0/CPU0:ios#show controllers coherentDSP 0/2/0/12
Thu Sep 30 14:17:04.411 UTC

Port                                          : CoherentDSP 0/2/0/12
Controller State                              : Up
Inherited Secondary State                     : Normal
Configured Secondary State                    : Maintenance
Derived State                                 : Maintenance
Loopback mode                                 : Internal
BER Thresholds                                : SF = 1.0E-5  SD = 1.0E-7
```

```
Performance Monitoring                          : Enable
Bandwidth                                       : 200.0Gb/s

Alarm Information:
LOS = 2 LOF = 0 LOM = 0
OOF = 1 OOM = 0 AIS = 1
IAE = 0 BIAE = 0        SF_BER = 0
SD_BER = 0      BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0     FLEXO_GIDM = 0
FLEXO-MM = 0    FLEXO-LOM = 0   FLEXO-RDI = 1
FLEXO-LOF = 0
Detected Alarms                                 : None

Bit Error Rate Information
PREFEC  BER                                     : 2.46E-08
POSTFEC BER                                     : 0.00E+00
Q-Factor                                        : 14.60 dB

Q-Margin                                        : 8.30dB

TTI :
        Remote hostname                         : ios
        Remote interface                        : CoherentDSP 0/2/0/12
        Remote IP addr                          : 0.0.0.0

FEC mode                                        : O_FEC

Flexo-Mode                                      : Enable
Flexo Details:
        Tx GID                                  : 1
        TX IID                                  : 1, 2,
        Rx GID                                  : 1
        RX IID                                  : 1, 2,

Flexo Peers Information:
        Controller                              : CoherentDSP0_2_0_13
        OTUCn rate                              : OTUC2


AINS Soak                                       : None
AINS Timer                                      : 0h, 0m
AINS remaining time                             : 0 seconds


RP/0/RP0/CPU0:ios#sh controllers coherentDSP 0/2/0/13
Thu Sep 30 14:17:08.140 UTC

Port                                            : CoherentDSP 0/2/0/13
Controller State                                : Up
Inherited Secondary State                       : Normal
Configured Secondary State                      : Maintenance
Derived State                                   : Maintenance
Loopback mode                                   : Internal
BER Thresholds                                  : SF = 1.0E-5  SD = 1.0E-7
Performance Monitoring                          : Enable
Bandwidth                                       : 200.0Gb/s

Alarm Information:
LOS = 1 LOF = 0 LOM = 0
OOF = 0 OOM = 0 AIS = 0
IAE = 0 BIAE = 0        SF_BER = 0
SD_BER = 0      BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0     FLEXO_GIDM = 0
FLEXO-MM = 0    FLEXO-LOM = 0   FLEXO-RDI = 1
```

```
FLEXO-LOF = 0
Detected Alarms                                 : None

Bit Error Rate Information
PREFEC  BER                                     : 0.00E+00
POSTFEC BER                                     : 0.00E+00
Q-Factor                                        : 15.70 dB

Q-Margin                                        : 9.50dB

TTI :
        Remote IP addr                          : 0.0.0.0

FEC mode                                        : O_FEC

Flexo-Mode                                      : Enable
Flexo Details:
        Tx GID                                  : 1
        TX IID                                  : 3, 4,
        Rx GID                                  : 1
        RX IID                                  : 3, 4,

Flexo Peers Information:
        Controller                              : CoherentDSP0_2_0_12
        OTUCn rate                              : OTUC2


AINS Soak                                       : None
AINS Timer                                      : 0h, 0m
AINS remaining time                             : 0 seconds
```

The following is a sample of an encryption configuration on an ODUC4 controller.

```
show controllers oduc4 0/0/0/12 otnsec

Wed Sep 28 23:17:15.395 UTC
Controller Name          : ODUC4 0/0/0/12
Source ip                : 10.1.1.1
Destination ip           : 10    .1.1.2
Session id               : 99
IKEv2 profile            : profile_all_in_one
Session State            : SECURED

Otnsec policy name       : otnsecpolicy1
  cipher-suite           : AES-GCM-256
  security-policy        : Must Secure
  sak-rekey-interval     : 120
Time to rekey            : 103
Time to Expire           : 1284201

Programming Status       :
  Inbound SA(Rx)         :
    AN[1]                :
        SPI              : 0x6301
  Outbound SA(Tx)        :
    AN[0]                :
        SPI              : None
    AN[1]                :
        SPI              : 0x6301
RP/0/RP0/CPU0:ios#
```

show access-lists ipv4

To display the contents of current IPv4 access lists, use the **show access-lists ipv4** command in EXEC mode.

show access-lists ipv4 [**interface MgmtEth** *R/S/I/P* | **maximum** [**detail**] | **summary** [*access-list-name*] | **usage pfilter location** { **location** *node-id* | **all** } | *access-list-name* [*sequence-number* | **usage pfilter location** { **location** *node-id* | **all** }]]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port/ number of the interface.
access-list-name	(Optional) Name of a particular IPv4 access list. The name cannot contain a space or quotation mark; it may contain numbers.
location *number*	Location of a particular IPv4 access list.
location*node-id*	(Optional) Location of a particular IPv4 access list. The node-id argument is entered in the rack/slot/module notation.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
summary	Displays a summary of all current IPv4 access lists.
sequence-number	(Optional) Sequence number of a particular IPv4 access list.
maximum	Displays the current maximum number of configurable IPv4 accesscontrol lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv4 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines

Use the **show access-lists ipv4** command to display the contents of all IPv4 access lists. To display the contents of a specific IPv4 access list, use the name argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **show access-lists ipv4 summary** command to display a summary of all current IPv4 access lists. To display a summary of a specific IPv4 access list, use the name argument.

Use the **show access-lists ipv4 maximum detail** command to display the OOR details for IPv4 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

Example

In the following example, the contents of all IPv4 access lists are displayed:

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

```
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)
```

show access-lists ipv6

To display the contents of current IPv6 access lists, use the **show access-lists ipv6** command in EXEC mode.

show access-lists ipv6 [**interface MgmtEth** *R/S/I/P* | **maximum** [**detail**] | **summary** [*access-list-name*] | **usage pfilter location** { **location** *node-id* | **all** } | *access-list-name* [*sequence-number* | **usage pfilter location** { **location** *node-id* | **all** }]]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port/ number of the interface.
access-list-name	(Optional) Name of a particular IPv4 access list. The name cannot contain a space or quotation mark; it may contain numbers.
location *number*	Location of a particular IPv4 access list.
location *node-id*	(Optional) Location of a particular IPv4 access list. The node-id argument is entered in the rack/slot/module notation.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
summary	Displays a summary of all current IPv4 access lists.
sequence-number	(Optional) Sequence number of a particular IPv4 access list.
maximum	Displays the current maximum number of configurable IPv4 accesscontrol lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv6 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines

The **show access-lists ipv6** command is similar to the **show access-lists ipv4** command, except that it is IPv6 specific.

Use the **show access-lists ipv6** command to display the contents of all IPv6 access lists. To display the contents of a specific IPv6 access list, use the name argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **show access-lists ipv6 summary** command to display a summary of all current IPv6 access lists. To display a summary of a specific IPv6 access list, use the name argument.

Use the **show access-lists ipv6 maximum detail** command to display the OOR details for IPv6 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

Example

In the following example, the contents of all IPv6 access lists are displayed:

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

```
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)
```

show environment

To display environmental monitor parameters for the system, use the **show environment** command in administration EXEC mode.

show environment [**all** | **fan** | **power** | **voltages** | **current** | **trace** | **temperatures**] [**location** | *location*]

Syntax Description

all	(Optional) Displays information for all the environmental monitor parameters.
fan	(Optional) Displays information about the fans.
power	(Optional) Displays power supply voltage and current information.
voltages	(Optional) Displays system voltage information.
current	(Optional) Displays current sensor information.
temperatures	(Optional) Displays system temperature information.

trace	(Optional) Displays trace data for environment monitoring.
location | *location*	(Optional) Enter the location for which the environmental information needs to be displayed.

Command Default

All environmental monitor parameters are displayed.

Command Modes

Administration EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show environment** command displays information about the hardware that is installed in the system, including fans, power supply voltage, current information, and temperatures.

Example

The following example shows sample output from the **show environment** command with the **fan** keyword.

sysadmin-vm:0_RP0# **show environment fan**

```
Wed Mar  20 04:40:02.510 UTC+00:00
=============================================
                        Fan speed (rpm)
Location     FRU Type           FAN_0   FAN_1
---------------------------------------------
0/FT0        NCS1K4-FAN          7020    6960
0/FT1        NCS1K4-FAN          6750    6720
0/FT2        NCS1K4-FAN          6750    6720

0/PM0        NCS1K4-AC-PSU      24800   23680

0/PM1        NCS1K4-AC-PSU      14240   14176
```

The following example shows sample output from the **show environment** command with the **temperatures** keyword.

sysadmin-vm:0_RP0# **show environment temperatures location 0/RP0**

```
Wed Mar  20 04:40:48.518 UTC+00:00
================================================================================
Location  TEMPERATURE                Value   Crit Major Minor Minor Major  Crit
          Sensor                   (deg C)   (Lo) (Lo)   (Lo)   (Hi)   (Hi)   (Hi)
--------------------------------------------------------------------------------
0/RP0
          TEMP_LOCAL                  29    -10    -5     0     55     65     70
          TEMP_REMOTE1                30    -10    -5     0     55     65     70
          TEMP_CPU_DIE                30    -10    -5     0     75     80     90
```

The following example shows sample output from the **show environment** command with the **power** keyword.

sysadmin-vm:0_RP0# **show environment power**

```
Wed Mar  20 04:41:39.990 UTC+00:00
================================================================================
CHASSIS LEVEL POWER INFO: 0
================================================================================
   Total output power capacity (N + 1)             :    2000W +       0W
   Total output power required                     :    1430W
   Total power input                               :    1075W
   Total power output                              :    1009W

Power Group 0:
================================================================================
   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
================================================================================
   0/PM0       2kW-AC        0.0      0.0      0.0      0.0    FAILED or NO PWR

Total of Power Group 0:          0W/  0.0A         0W/  0.0A

Power Group 1:
================================================================================
   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
================================================================================
   0/PM1       2kW-AC      228.8      4.7     12.1     83.4    OK

Total of Power Group 1:       1075W/  4.7A      1009W/ 83.4A

================================================================================
   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts
================================================================================
   0/0          NCS1K4-1.2T-K9         260           -       ON
   0/1          NCS1K4-1.2T-K9         260           -       ON
   0/2          NCS1K4-1.2T-K9         260           -       ON
   0/3          NCS1K4-1.2T-K9         260           -       ON
   0/RP0        NCS1K4-CNTLR-K9         55           -       ON
   0/FT0        NCS1K4-FAN             100           -       ON
   0/FT1        NCS1K4-FAN             100           -       ON
   0/FT2        NCS1K4-FAN             100           -       ON
   0/SC0        NCS1004                 35           -       ON
```

The following example shows sample output from the **show environment** command with the **voltages** keyword.

sysadmin-vm:0_RP0# **show environment voltages location 0/RP0**

```
Wed Mar  20 04:43:04.524 UTC+00:00
================================================================================
Location  VOLTAGE                      Value   Crit Minor Minor  Crit
          Sensor                       (mV)    (Lo) (Lo)  (Hi)   (Hi)
--------------------------------------------------------------------------------
0/RP0
          ADM1266_VH1_12V             11982  10800 11040 12960 13200
          ADM1266_VH3_3V3              3303   3036  3135  3465  3564
          ADM1266_VH4_2V5              2493   2300  2375  2625  2700
          ADM1266_VP1_1V8              1794   1656  1710  1890  1944
          ADM1266_VP2_1V2              1189   1104  1140  1260  1296
          ADM1266_3V3_STAND_BY         3303   3036  3135  3465  3564
          ADM1266_VP4_3V3_CPU          3301   3036  3135  3465  3564
          ADM1266_VP5_2V5_CPU          2490   2300  2375  2625  2700
          ADM1266_VP6_1V8_CPU          1796   1656  1710  1890  1944
          ADM1266_VP7_1V24_VCCREF      1233   1140  1178  1302  1339
```

```
ADM1266_VP8_1V05_CPU          1047    966   997  1102  1134
ADM1266_VP9_1V2_DDR_VDDQ      1200   1104  1140  1260  1296
ADM1266_VP10_1V0_VCCRAM       1056    500   650  1300  1400
ADM1266_VP11_VNN               876    400   550  1300  1400
ADM1266_VP12_VCCP             1062    300   450  1300  1400
ADM1266_VP13_0V6_VTT           600    552   570   630   648
ADM1293_DB_5V0                5014   4600  4750  5250  5400
ADM1293_DB_3V3                3317   3036  3135  3465  3564
ADM1293_DB_5V0_USB_0          5018   4000  4500  5500  6000
ADM1293_DB_5V0_USB_1          5036   4000  4500  5500  6000
ADM1293_MB_5V0_PMOD0          4932   4600  4750  5250  5400
ADM1293_MB_5V0_PMOD1          5012   4600  4750  5250  5400
ADM1293_MB_2V5_PLL            2485   2300  2375  2625  2700
```

show hw-module

To display the details of the muxponder slice, Field Programmable Devices (FPDs), and the card configuration in regen mode, use the **show hw-module** in XR EXEC or administration EXEC mode.

show hw-module { **fpd** | **location** *location* [**mxponder** | **mxponder-slice** | **regen** | **xponder capabilities**] }
slicenumber

Syntax Description

fpd	Displays the status of FPDs installed.
location *location*	Specifies the location.
mxponder	Displays information for all the slices of the muxponder.
mxponder-slice *slicenumber*	Displays information for a specific slice of the muxponder. The valid values of *slicenumber* are 0 and 1.
regen	Displays information of card configuration in regen mode.
xponder capabilities	Displays the client ports that are mapped to each trunk port along with the corresponding trunk rates and client rates.

Command Default

None

Command Modes

XR EXEC

Administration EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.1.1	**regen** keyword was added.
Release 7.3.2	**xponder capabilities** keyword was added.

Usage Guidelines

If the ISO image has new version of FPD, the Status column in **show hw-module fpd** command shows NEED UPGD. If the upgrade is required, use the **upgrade hw-module location all fpd *fpd_device_name*** command to start the upgrade. When the upgrade starts, the Status column in **show hw-module fpd** command sequentially shows UPGD PREP, UPGRADING, and the percentage of upgrade completion. After the upgrade is completed, the Status column shows RLOAD REQ if the ISO image requires reload; otherwise the Status column shows CURRENT.



Note The upgrade of LC_OPT_MOD_FW FPD affects traffic. Hence, the user must perform this upgrade during a maintenance window.

If reload is required:

Reload the line card or use the **admin hw-module location all reload** command to reboot NCS 1004. After the reload is completed, the new FPGA runs the current version.

Example

```
RP/0/RP0/CPU0:ios#show hw-module location 0/2 mxponder
Fri Mar 15 11:48:48.344 IST

Location:             0/2
Client Bitrate:       100GE
Trunk  Bitrate:       500G
Status:               Provisioned
LLDP Drop Enabled:    FALSE
Client Port                     Mapper/Trunk Port          CoherentDSP0/2/0/0
CoherentDSP0/2/0/1
                                Traffic Split Percentage

HundredGigECtrlr0/2/0/2         ODU40/2/0/0/1                       100
    0
HundredGigECtrlr0/2/0/3         ODU40/2/0/0/2                       100
    0
HundredGigECtrlr0/2/0/4         ODU40/2/0/0/3                       100
    0
HundredGigECtrlr0/2/0/5         ODU40/2/0/0/4                       100
    0
HundredGigECtrlr0/2/0/6         ODU40/2/0/0/5                       100
    0
HundredGigECtrlr0/2/0/7         ODU40/2/0/1/1                         0
  100
HundredGigECtrlr0/2/0/8         ODU40/2/0/1/2                         0
  100
HundredGigECtrlr0/2/0/9         ODU40/2/0/1/3                         0
  100
HundredGigECtrlr0/2/0/10        ODU40/2/0/1/4                         0
  100
HundredGigECtrlr0/2/0/11        ODU40/2/0/1/5                         0
  100
```

The following is a sample output of all the muxponder slice 0 configurations.

```
RP/0/RP0/CPU0:ios#show hw-module location 0/1 mxponder-slice 0
Fri Mar 15 06:04:18.348 UTC

Location:             0/1
```

```
Slice ID:             0
Client Bitrate:       100GE
Trunk  Bitrate:       500G
Status:               Provisioned
LLDP Drop Enabled:    FALSE
Client Port                    Mapper/Trunk Port          CoherentDSP0/1/0/0
                               Traffic Split Percentage

HundredGigECtrlr0/1/0/2        ODU40/1/0/0/1                      100
HundredGigECtrlr0/1/0/3        ODU40/1/0/0/2                      100
HundredGigECtrlr0/1/0/4        ODU40/1/0/0/3                      100
HundredGigECtrlr0/1/0/5        ODU40/1/0/0/4                      100
HundredGigECtrlr0/1/0/6        ODU40/1/0/0/5                      100
```

The following is a sample output of all the muxponder slice 1 configurations.

```
RP/0/RP0/CPU0:ios#show hw-module location 0/1 mxponder-slice 1
Fri Mar 15 06:11:50.020 UTC

Location:             0/1
Slice ID:             1
Client Bitrate:       100GE
Trunk  Bitrate:       400G
Status:               Provisioned
LLDP Drop Enabled:    TRUE
Client Port                    Mapper/Trunk Port          CoherentDSP0/1/0/1
                               Traffic Split Percentage

HundredGigECtrlr0/1/0/8        ODU40/1/0/1/1                      100
HundredGigECtrlr0/1/0/9        ODU40/1/0/1/2                      100
HundredGigECtrlr0/1/0/10       ODU40/1/0/1/3                      100
HundredGigECtrlr0/1/0/11       ODU40/1/0/1/4                      100
```

The following is a sample output of card configuration in regen mode.

```
RP/0/RP0/CPU0:ios#show hw-module location 0/0 regen
Mon Mar 25 09:50:42.936 UTC

Location:             0/0
Trunk  Bitrate:       400G
Status:               Provisioned
East Port              West Port
CoherentDSP0/0/0/0      CoherentDSP0/0/0/1
```

The following shows the muxponder slice 0 configurations where the client ports that are mapped to each trunk port are displayed along with the corresponding trunk rates and client rates.

```
RP/0/RP0/CPU0:ios#show hw-module location 0/1 xponder-capabilities mxponder-slice 0
Fri Aug 13 18:21:43.931 UTC

Location: 0/1

Trunk-Port(s): 11

Port Group Restrictions:
Shared-Client-Group-Bandwidth Shared-Group-Client-Ports
400G 1, 6, 7, 10

Trunk-bandwidth: 400G
Client-port Supported client rates
1 100GE
6 100GE
7 100GE
```

```
10 100GE

Trunk-bandwidth: 300G
Client-port Supported client rates
1 100GE
7 100GE
10 100GE

Trunk-bandwidth: 200G
Client-port Supported client rates
7 100GE
10 100GE
```

show inventory

To retrieve and display the physical inventory information, use the **show inventory** command in XR EXEC or administration EXEC mode.

XR EXEC Mode

show inventory [**all** | **oid** | **raw** | **location** *location*]

Administration EXEC Mode

show inventory [**all** | **chassis** | **fan** | **power** | **raw** | **location** *location*]

Syntax Description

all	(Optional) Displays inventory information for all the physical entities.
fan	(Optional) Displays inventory information for the fans.
power	(Optional) Displays inventory information for the power supply.
raw	(Optional) Displays raw information about the chassis for diagnostic purposes.
chassis	(Optional) Displays inventory information for the entire chassis.
location *location*	(Optional) Displays inventory information for a specific node, or for all nodes in the chassis.
oid	(Optional) Displays inventory information along with oid.

Command Default

All hardware inventory information is displayed.

Command Modes

XR EXEC

Administration EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Enter the **show inventory** command with the **raw** keyword to display every RFC 2737 entity installed in NCS 1004, including those without a PID, unique device identifier (UDI), or other physical identification. The **raw** keyword is primarily intended for troubleshooting problems with the **show inventory** command itself.

Example

The following examples show sample output from the **show inventory** command in both EXEC and Administration EXEC modes.

sysadmin-vm:0_RP0# **show inventory**

```
Thu Mar  7  12:49:15.974 UTC+00:00

 Name: Rack 0               Descr: Network Convergence System 1004 Chassis
 PID: NCS1004               VID: V00                  SN: CAT2217B020

 Name: 0/0-Optics0/0/0/2    Descr: Cisco QSFP-100G-LR4-S Pluggable Optics Module
 PID: QSFP-100G-LR4-S       VID: V01                  SN: FNS20530F3H

 Name: 0/0-Optics0/0/0/3    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: JFQ22108035

 Name: 0/0-Optics0/0/0/4    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: JFQ22108033

 Name: 0/0-Optics0/0/0/5    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150QF8

 Name: 0/0-Optics0/0/0/6    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150UJQ

 Name: 0/0-Optics0/0/0/7    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150Q9P

 Name: 0/0-Optics0/0/0/8    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150TE5

 Name: 0/0-Optics0/0/0/9    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150TCP

 Name: 0/0-Optics0/0/0/10   Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150LDS

 Name: 0/0-Optics0/0/0/11   Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150L5H

 Name: 0/0-Optics0/0/0/12   Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150SED

 Name: 0/0-Optics0/0/0/13   Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150TUV

 Name: 0/0                  Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
 PID: NCS1K4-1.2T-K9        VID: V00                  SN: CAT2250B0A9

 Name: 0/1-Optics0/1/0/2    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: JFQ22108003

 Name: 0/1-Optics0/1/0/3    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S     VID: V02                  SN: FNS22150QD8
```

```
 Name: 0/1-Optics0/1/0/4     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ22108004

Name: 0/1-Optics0/1/0/5     Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR        VID: V02                   SN: FNS22070GFW

 Name: 0/1-Optics0/1/0/6     Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR        VID: V01                   SN: FNS20510ZFP

 Name: 0/1-Optics0/1/0/7     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: FNS22150QFJ

 Name: 0/1-Optics0/1/0/8     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: FNS22150TZF

 Name: 0/1-Optics0/1/0/9     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: FNS22150UJS

 Name: 0/1-Optics0/1/0/10    Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR        VID: V02                   SN: FNS22070GCH

 Name: 0/1-Optics0/1/0/11    Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR        VID: V02                   SN: FNS22070J79

 Name: 0/1-Optics0/1/0/12    Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR        VID: V02                   SN: FNS22070GD7

 Name: 0/1-Optics0/1/0/13    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: FNS22150LHE

 Name: 0/1                   Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
 PID: NCS1K4-1.2T-K9         VID: V00                   SN: CAT2223B129

 Name: 0/2-Optics0/2/0/2     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ22108001

 Name: 0/2-Optics0/2/0/3     Descr: Non-Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: LQ210CR-CPA1           VID: 01                    SN: FG4657250006

 Name: 0/2-Optics0/2/0/4     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210802P

 Name: 0/2-Optics0/2/0/5     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210802Q

 Name: 0/2-Optics0/2/0/6     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210802R

 Name: 0/2-Optics0/2/0/7     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210802U

 Name: 0/2-Optics0/2/0/8     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2146802T

 Name: 0/2-Optics0/2/0/9     Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210800G

 Name: 0/2-Optics0/2/0/10    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210802M

 Name: 0/2-Optics0/2/0/11    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210800P

 Name: 0/2                   Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card - Licensed
```

```
 PID: NCS1K4-1.2T-L-K9       VID: V00                  SN: CAT2250B09F

 Name: 0/3-Optics0/3/0/2     Descr: Non-Cisco 100G QSFP28 LR4 Pluggable Optics Module
 PID: ONS-QSFP28-LR4         VID: V01                  SN: FNS20500RVT

 Name: 0/3-Optics0/3/0/3     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S1D4

 Name: 0/3-Optics0/3/0/4     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S16R

 Name: 0/3-Optics0/3/0/5     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S16W

 Name: 0/3-Optics0/3/0/6     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S17H

 Name: 0/3-Optics0/3/0/7     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S1BA

 Name: 0/3-Optics0/3/0/8     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S16G

 Name: 0/3-Optics0/3/0/9     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S17N

 Name: 0/3-Optics0/3/0/10    Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S15W

 Name: 0/3-Optics0/3/0/11    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                  SN: FNS22150TES

 Name: 0/3-Optics0/3/0/12    Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S16S

 Name: 0/3-Optics0/3/0/13    Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S        VID: V03                  SN: AVF2219S178

 Name: 0/3                   Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
 PID: NCS1K4-1.2T-K9         VID: V00                  SN: CAT2236B01A

 Name: 0/RP0                 Descr: Network Convergence System 1004 Controller
 PID: NCS1K4-CNTLR-K9        VID: V00                  SN: CAT2217B09N

Name: 0/FT0                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V00                  SN: CAT2218B12J

 Name: 0/FT1                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V00                  SN: CAT2218B125

 Name: 0/FT2                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V00                  SN: CAT2218B124

 Name: 0/PM0                 Descr: Network Convergence System 1004 AC Power Supply Unit
 PID: NCS1K4-AC-PSU          VID: V00                  SN: POG2212CL12

 Name: 0/PM1                 Descr: Network Convergence System 1004 AC Power Supply Unit
 PID: NCS1K4-AC-PSU          VID: V00                  SN: POG2212CL2Q

 Name: 0/SC0                 Descr: Network Convergence System 1004 Chassis
 PID: NCS1004                VID: V00                  SN: CAT2217B020
```

RP/0/RP0/CPU0:ios# **show inventory**

```
Thu Mar  7 10:39:50.321 UTC
NAME: "0/0", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9    , VID: V00, SN: CAT2250B0A9

NAME: "0/0-Optics0/0/0/2", DESCR: "Cisco QSFP-100G-LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S   , VID: V01 , SN: FNS20530F3H

NAME: "0/0-Optics0/0/0/3", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ22108035

NAME: "0/0-Optics0/0/0/4", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ22108033

NAME: "0/0-Optics0/0/0/5", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150QF8

NAME: "0/0-Optics0/0/0/6", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150UJQ

NAME: "0/0-Optics0/0/0/7", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150Q9P

NAME: "0/0-Optics0/0/0/8", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150TE5

NAME: "0/0-Optics0/0/0/9", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150TCP

NAME: "0/0-Optics0/0/0/10", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150LDS

NAME: "0/0-Optics0/0/0/11", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150L5H

NAME: "0/0-Optics0/0/0/12", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150SED

NAME: "0/0-Optics0/0/0/13", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150TUV

NAME: "0/1", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9    , VID: V00, SN: CAT2223B129

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ22108003

NAME: "0/1-Optics0/1/0/3", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150QD8

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ22108004

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR   , VID: V02 , SN: FNS22070GFW

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR   , VID: V01 , SN: FNS20510ZFP

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150QFJ

NAME: "0/1-Optics0/1/0/8", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150TZF
```

```
NAME: "0/1-Optics0/1/0/9", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150UJS

NAME: "0/1-Optics0/1/0/10", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR   , VID: V02 , SN: FNS22070GCH

NAME: "0/1-Optics0/1/0/11", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR   , VID: V02 , SN: FNS22070J79

NAME: "0/1-Optics0/1/0/12", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR   , VID: V02 , SN: FNS22070GD7

NAME: "0/1-Optics0/1/0/13", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150LHE

NAME: "0/2", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card - Licensed"
PID: NCS1K4-1.2T-L-K9  , VID: V00, SN: CAT2250B09F

NAME: "0/2-Optics0/2/0/2", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ22108001

NAME: "0/2-Optics0/2/0/3", DESCR: "Non-Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: LQ210CR-CPA1      , VID: 01 , SN: FG4657250006

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2210802P

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2210802Q

NAME: "0/2-Optics0/2/0/6", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2210802R

NAME: "0/2-Optics0/2/0/7", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2210802U

NAME: "0/2-Optics0/2/0/8", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2146802T

NAME: "0/2-Optics0/2/0/9", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2210800G

NAME: "0/2-Optics0/2/0/10", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2210802M

NAME: "0/2-Optics0/2/0/11", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: JFQ2210800P

NAME: "0/3", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9    , VID: V00, SN: CAT2236B01A

NAME: "0/3-Optics0/3/0/2", DESCR: "Non-Cisco 100G QSFP28 LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01 , SN: FNS20500RVT

NAME: "0/3-Optics0/3/0/3", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S1D4

NAME: "0/3-Optics0/3/0/4", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S16R

NAME: "0/3-Optics0/3/0/5", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S16W
```

```
NAME: "0/3-Optics0/3/0/6", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S17H

NAME: "0/3-Optics0/3/0/7", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S1BA

NAME: "0/3-Optics0/3/0/8", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S16G

NAME: "0/3-Optics0/3/0/9", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S17N

NAME: "0/3-Optics0/3/0/10", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S15W

NAME: "0/3-Optics0/3/0/11", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V02 , SN: FNS22150TES

NAME: "0/3-Optics0/3/0/12", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S16S

NAME: "0/3-Optics0/3/0/13", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S   , VID: V03 , SN: AVF2219S178

NAME: "0/RP0", DESCR: "Network Convergence System 1004 Controller"
PID: NCS1K4-CNTLR-K9   , VID: V00, SN: CAT2217B09N

NAME: "0/SC0", DESCR: "Network Convergence System 1004 Chassis"
PID: NCS1004           , VID: V00, SN: CAT2217B020

NAME: "Rack 0", DESCR: "Network Convergence System 1004 Chassis"
PID: NCS1004           , VID: V00, SN: CAT2217B020

NAME: "0/FT0", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V00, SN: CAT2218B12J

NAME: "0/FT1", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V00, SN: CAT2218B125

NAME: "0/FT2", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V00, SN: CAT2218B124

NAME: "0/PM0", DESCR: "Network Convergence System 1004 AC Power Supply Unit           "
PID: NCS1K4-AC-PSU     , VID: V00, SN: POG2212CL12

NAME: "0/PM1", DESCR: "Network Convergence System 1004 AC Power Supply Unit           "
PID: NCS1K4-AC-PSU     , VID: V00, SN: POG2212CL2Q
```

show lc-module (OTN-XP Card)

To display the details of the LC mode configured on the OTN-XP card, use the **show lc-module** in XR EXEC or administration EXEC mode.

show lc-module location *location* **lcmode** [**all**]

Syntax Description

location *location*	Specifies the location.
lcmode	Displays the LC mode configured.

all	Displays all type of LC modes that are supported on the OTN-XP card.

Command Default

None

Command Modes

XR EXEC

Administration EXEC

Command History

Release	Modification
Release 7.2.1	This command was introduced.

The following sample displays the LC modes that are configured on the OTN-XP card.

```
RP/0/RP0/CPU0:ios#show lc-module location 0/3 lcmode all
Wed Aug 11 17:06:29.538 UTC
States: A-Available R-Running C-Configured
Node   Lcmode_Supported     Owner   Options(State)            HW_Ver
------------------------------------------------------------------------------
0/3         Yes              CLI     10G-GREY-MXP (A)          3.0
                                     4x100G-MXP-400G-TXP (A)   2.0
                                     40x10G-4x100G-MXP (A)     3.0
                                     4x100GE-MXP-DD (R/C)      7.0
```

The following sample displays the OTUCn-REGEN LC mode that is configured on the OTN-XP card.

```
RP/0/RP0/CPU0:ios#show lc-module location 0/2 lcmode
Fri Feb  4 17:00:09.842 UTC

Node    Lcmode_Supported    Owner      Running          Configured
-------------------------------------------------------------------------------------------------
0/2       Yes                CLI       OTUCn-REGEN       OTUCn-REGEN
```

The following sample displays the FC-MXP LC mode that is configured on the OTN-XP card.

```
RP/0/RP0/CPU0:ios#show lc-module location 0/2 lcmode
Fri Feb  4 17:00:09.842 UTC

Node    Lcmode_Supported    Owner      Running          Configured
-------------------------------------------------------------------------------------------------
0/2       Yes                CLI       OTUCn-REGEN       FC-MXP
```

show led

To display the status of various LEDs present in NCS 1004, use the **show led** command in administration EXEC mode.

show led [**location** *location*]

Syntax Description

location *location*	(Optional) Displays LED information for a specific location.

Command Default

The status of all the LEDs present in NCS 1004 is displayed.

Command Modes Administration EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines Enter the **show LED** command in administration EXEC mode to display the status of all the LEDs present in NCS 1004.

Example

The following example shows sample output from the **show led** command.

sysadmin-vm:0_RP0# **show led**

```
Wed Mar  20 04:45:25.457 UTC+00:00
==============================================================
Location  LED Name                       Mode          Color
==============================================================
0/0
          0/0-Status LED                 WORKING     GREEN
0/1
          0/1-Status LED                 WORKING     GREEN
0/2
          0/2-Status LED                 WORKING     GREEN
0/3
          0/3-Status LED                 WORKING     GREEN
0/RP0
          0/RP0-Attention LED            WORKING     OFF
          0/RP0-SYS LED                  WORKING     AMBER
          0/RP0-PSU LED                  WORKING     RED
          0/RP0-FAN LED                  WORKING     GREEN
0/FT0
          0/FT0-Status LED               WORKING     GREEN
0/FT1
          0/FT1-Status LED               WORKING     GREEN
0/FT2
          0/FT2-Status LED               WORKING     GREEN
0/PM0
          0/PM0-Status LED               WORKING     AMBER
0/PM1
          0/PM1-Status LED               WORKING     GREEN
```

show platform

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

Administration EXEC Mode

show platform [{**detail** | **location** | **slices**} *location*]

XR EXEC Mode

show platform [**vm** | **0/RP0**]

Syntax Description

detail	(Optional) Displays the details of node type and state.
location	(Optional) Displays the location of node.
slices	(Optional) Displays the summary information of each slice in the node.
location	(Optional) Node location such as 0/FT0, 0/RP0.
vm	(Optional) Displays the virtual machine information of node.

Command Default

The status and information are displayed for all the nodes in the system.

Command Modes

XR EXEC

Administration EXEC

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Enter the **show platform** command in administration EXEC mode to display the output for the entire system.

Example

The following example shows sample output from the **show platform** command.

sysadmin-vm:0_RP0# **show platform**

```
Wed Mar  20 04:27:21.562 UTC+00:00
Location  Card Type              HW State      SW State      Config State
------------------------------------------------------------------------------
0/0       NCS1K4-1.2T-K9         OPERATIONAL   N/A           NSHUT
0/1       NCS1K4-1.2T-K9         OPERATIONAL   N/A           NSHUT
0/2       NCS1K4-1.2T-K9         OPERATIONAL   N/A           NSHUT
0/3       NCS1K4-1.2T-K9         OPERATIONAL   N/A           NSHUT
0/RP0     NCS1K4-CNTLR-K9        OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NCS1K4-FAN             OPERATIONAL   N/A           NSHUT
0/FT1     NCS1K4-FAN             OPERATIONAL   N/A           NSHUT
0/FT2     NCS1K4-FAN             OPERATIONAL   N/A           NSHUT
0/PM0     NCS1K4-AC-PSU          OPERATIONAL   N/A           NSHUT
0/PM1     NCS1K4-AC-PSU          OPERATIONAL   N/A           NSHUT
0/SC0     NCS1004                OPERATIONAL   N/A           NSHUT
```

The following example shows sample output from the **show platform detail** command.

sysadmin-vm:0_RP0# **show platform detail**

```
Wed Mar  20 04:31:02.480 UTC+00:00
MODULE
              HW OPER      SW OPER
LOCATION :  PID :            DESCRIPTION :
    VID/SN :  STATE :      STATE :      CONFIGURATION :  HW VERSION :  LAST  EVENT :
LAST  EVENT  REASON :
```

```
0/0          NCS1K4-1.2T-K9   NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW READY
0/1          NCS1K4-1.2T-K9   NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW READY
0/2          NCS1K4-1.2T-K9   NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW READY
0/3          NCS1K4-1.2T-K9   NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW READY
0/RP0        NCS1K4-CNTLR-K9  Network Convergence System 1004 Controller
    V00        OPERATIONAL  OPERATIONAL  NSHUT RST        0.1           HW_EVENT_OK
HW Event OK
0/FT0        NCS1K4-FAN       Network Convergence System 1004 Fan
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW Operational
0/FT1        NCS1K4-FAN       Network Convergence System 1004 Fan
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW Operational
0/FT2        NCS1K4-FAN       Network Convergence System 1004 Fan
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW Operational
0/PM0        NCS1K4-AC-PSU    Network Convergence System 1004 AC Power Supply Unit
    V00        OPERATIONAL  N/A          NSHUT RST        0.0           HW_EVENT_OK
HW Operational
0/PM1        NCS1K4-AC-PSU    Network Convergence System 1004 AC Power Supply Unit
    V00        OPERATIONAL  N/A          NSHUT RST        0.0           HW_EVENT_OK
HW Operational
0/SC0        NCS1004          Network Convergence System 1004 Chassis
    V00        OPERATIONAL  N/A          NSHUT RST        0.1           HW_EVENT_OK
HW Event OK
```

RP/0/RP0/CPU0:ios# **show platform**

```
Wed Mar 20 04:23:12.582 UTC
Node              Type                        State             Config state
--------------------------------------------------------------------------------
0/0               NCS1K4-1.2T-K9              OPERATIONAL       NSHUT
0/1               NCS1K4-1.2T-K9              OPERATIONAL       NSHUT
0/2               NCS1K4-1.2T-K9              OPERATIONAL       NSHUT
0/3               NCS1K4-1.2T-K9              OPERATIONAL       NSHUT
0/RP0/CPU0        NCS1K4-CNTLR-K9(Active)     IOS XR RUN        NSHUT
0/FT0             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/FT1             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/FT2             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/PM0             NCS1K4-AC-PSU               OPERATIONAL       NSHUT
0/PM1             NCS1K4-AC-PSU               OPERATIONAL       NSHUT
0/SC0             NCS1004                     OPERATIONAL       NSHUT
```

show tcp dump-file

To display the details of the PCB state from a dump file, use the **show tcp dump-file** command in in EXEC mode.

show tcp dump-file { *dump-file-name* | | **all** | | **list** | { *ipv4-address-of-dumpfiles* | *ipv6-address-of-dumpfiles* | | **all** } } { **location** *node-id* }

Syntax Description

all	Displays all connections information.
location *node-id*	Displays RAW statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release R24.2.1	This command was introduced.

Usage Guidelines

The basic use of this command is to provide information about the list of all TCP dump files, details of any specific or all TCP dumpfile file. You can also use this command for debugging purpose or to monitor the flow of TCP packets for a TCP connection.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp dumpfile all location 0/RP0/CPU0** command:

```
RP/0/RP0/CPU0:ios# show tcp dumpfile list all location 0/RP0/CPU0

total 4
-rw-r--r-- 1 rpathark eng 3884 May 11 20:16 80_80_80_80.26355.179.cl.15892
```

show type6

To view Type 6 password encryption information, use the **show type6** command in EXEC mode.

show type6 [**server**]

Syntax Description

server	Displays Type 6 server information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XR Release 7.0.1	This command was introduced.

Usage Guidelines None

Example

The following command displays Type 6 password encryption feature information:

```
RP/0/RP0/CPU0:ios#show type6 server
Thu Jul 11 09:43:36.103 UTC
Server detail information:
==========================================
AES config State       :             Enabled
Masterkey config State :             Enabled
Type6 feature State    :             Enabled
Master key Inprogress  :             No
Masterkey Last updated/deleted :     Thu Jul 11 09:40:57 2024
```

signalling refresh out-of-band interval

To specify the out-of-band refresh interval for RSVP, use the **signalling refresh out-of-band interval** command in RSVP controller configuration mode.

signalling refresh out-of-band interval *interval*

Syntax Description

interval	Specifies the refresh interval (180-86400 seconds).

Command Default 45 seconds

Command Modes RSVP controller configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines This command applies only to the RSVP sessions associated with GMPLS UNI tunnels.

Example

The following example shows how to specify 200 seconds for the out-of-band interface refresh interval.

```
RP/0/RP0/CPU0:ios(config)#rsvp
RP/0/RP0/CPU0:ios(config-rsvp)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-rsvp-ctrl)#signalling refresh out-of-band interval 200
RP/0/RP0/CPU0:ios(config-rsvp-ctrl)#
```

signalling refresh out-of-band missed

To specify the number of missed refresh messages allowed before states are deleted for optical tunnels, use the **signalling refresh out-of-band missed** command in RSVP controller configuration mode.

signalling refresh out-of-band missed *mis-count*

Syntax Description

mis-count	Number of missed refresh messages allowed before states are deleted for optical tunnels (1-48).

Command Default

The default value is 12.

Command Modes

RSVP controller configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Usage Guidelines

This command applies only to the RSVP sessions associated with GMPLS UNI tunnels.

Example

The following example shows how to specify a maximum of 10 messages for the number of allowed missed refresh messages.

```
RP/0/RP0/CPU0:ios(config)#rsvp
RP/0/RP0/CPU0:ios(config-rsvp)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-rsvp-ctrl)#signalling refresh out-of-band missed 10
RP/0/RP0/CPU0:ios(config-rsvp-ctrl)#
```

sks profile

To configure the Session Key Service (SKS) profile with the IP address of the Key Management Entity (KME) server that manages cryptographic keys (dynamic Postquantum Preshared Keys (PPK), use the command **sks profile**.

sks profile *profile-name* **type** { **local | remote** } **kme server** **ipv4** *ipv4 adress* **port** *port number*

Syntax Description

profile-name	Name of the sks profile used in the dynamic PPK configuration.
type	Configures the type of the server.
local | remote	Indicates whether the server is local or remote server.
kme server ipv4	Configures the kme server IP address.
ipv4 adress	IP address of the kme server.

port	Configures the specific port number of the server, through which packets will be sent.
port number	Port number of the server.

Command Modes

Configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced

Example

The following example shows how to define a sks profile for dynamic ppk based IKEv2 encryption.

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/1/CPU0:ios(config)#sks profile qkd type remote
RP/0/1/CPU0:ios(config-sks-profile)#kme server ipv4 192.0.2.34 port 10001
RP/0/RP0/CPU0:ios(config-ikev2-keyring-peer)#exit
RP/0/RP0/CPU0:ios(config)#exit
```

split-client-port-mapping

To configure the trunk port to client port mapping for sub 50G configuration in the split client port mapping mode, use the **split-client-port-mapping** command in muxponder hardware module configuration mode.

split-client-port-mapping
no split-client-port-mapping

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default.

Command Modes

Muxponder hardware module configuration mode (config-hwmod-mxp)

Command History

Release	Modification
Release 7.5.2	This command is introduced.

Example

The following is a sample in which split-client-port-mapping is configured with a 450G trunk payload.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#trunk-rate 450G
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#client-rate 100GE
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#split-client-port-mapping
```

```
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#end
```

The following is a sample in which split client port-mapping configuration is removed.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module location 0/1 mxponder
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#no split-client-port-mapping
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#commit
RP/0/RP0/CPU0:ios(config-hwmod-mxp)#end
```

subject-name (trustpoint)

To specify the subject name in the certificate request, use the **subject-name** command in trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [**ca-certificate**] *subject-name*

Syntax Description

ca-certificate	(Optional) Specifies the subject name for the CA certificate for self-enrollment.
subject-name	(Optional) Specifies the subject name used in the certificate request.

Command Default

If the *subject-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, is used.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Before you can use the **subject-name** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that NCS 1004 should use and enters trustpoint configuration mode.

The **subject-name** command is an attribute that can be set for automatic enrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to specify the subject name for the frog certificate:

```
RP/0/0RP0RSP0/CPU0:ios# configure
RP/0/0RP0RSP0/CPU0:ios(config)# crypto ca trustpoint frog
RP/0/0RP0RSP0/CPU0:ios(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/0RP0RSP0/CPU0:ios(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/0RP0RSP0/CPU0:ios(config-trustp)# ip-address 172.19.72.120
```

This example shows how to specify the subject name for the CA certificate for self-enrollment.

```
RP/0/0RP0RSP0/CPU0:ios#configure
RP/0/0RP0RSP0/CPU0:ios(config)#crypto ca trustpoint system-trustpoint
RP/0/0RP0RSP0/CPU0:ios(config-trustp)#subject-name ca-certificate
CN=labuser-ca,C=US,ST=CA,L=San Jose,O=cisco systems,OU=ASR
RP/0/0RP0RSP0/CPU0:ios(config-trustp)#commit
```

ssh server timeout

To configure timeout for unused SSH connections and SSH channels on your routers that function as SSH servers, use the **ssh server timeout** command in configuration mode. To remove the timeout configuration, use the **no** form of this command.

ssh server timeout { **channel** | **connection** } *timeout-period*
no ssh server timeout

Syntax Description

ssh server timeout { **channel** | **connection** }	Configures server timeout for SSH channel and connection
timeout-period	Timeout period, in seconds, for unused SSH connections and idle SSH channels. The range is 1 to 86400.

Command Default

Disabled

Command Modes

Configuration mode

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

The unused connection timeout and channel timeout are applicable only for connections that are newly created after the timeout period is configured.

The channel timeout begins counting down after the set period of inactivity. The unused connection timeout begins counting down when there is no active channel within the SSH connection.

Task ID

Task ID	Operation
crypto	read, write

Examples

This example shows how to configure a timeout of 600 seconds for an unused SSH connection:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#ssh server timeout connection 600
RP/0/RP0/CPU0:ios(config-ssh)#commit
```

This example shows how to configure a timeout of 300 seconds for an idle SSH channel:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#ssh server timeout channel 300
RP/0/RP0/CPU0:ios(config-ssh)#commit
```

tcp dump-file convert

Use the **tcp dump-file convert** command in EXEC mode to convert the TCP dump packet traces files to other readable formats such as pcap, text, or both.

tcp dump-file convert { *pcap* | *text* | *all-formats* } { *all* | *binary_file_name* | *ipaddress* } **location** { *node-id* } **file** { *absolute file path* }

Syntax Description

pcap	Converts TCP dump packet files to packet capture (pcap) format.
text	Converts TCP dump packet traces files to text format.
all-format	Converts TCP dump packet traces files to both pcap and text format.
all	Collects TCP dump file data from all peers and nodes.
binary_file_name	Specifies the name of the dump file to be converted.
ipaddress	Specifies the IP address of the peer node.
location {*node-id*}	(Optional) Specifies the node to store the converted TCP dump file. The *node-id* is entered in the *rack/slot/module* notation, for example **location** *0/RP0/CPU0*. By default, the files are stored in the current node where the CLI command is executed.
file {*absolute file path* }	(Optional) Specifies the absolute file path where you want to store the converted TCP dump files. The file path is entertered in the *node/filename* notation, for example */harddisk:/demo1*. By default, the converted files are stored inside the file "decoded_dumpfiles" in the current node where the CLI command is executed or if you have provided the location the files are stored in that location.

Command Default

By default, the converted files are stored inside the *decoded_dumpfiles* file.

Command Modes

EXEC

Command History

Release	Modification
Release R24.2.1	This command was introduced.

Usage Guidelines

Use this command to convert TCP dump packet traces files into text, pcap, or both readable formats.

Examples

The following example shows how to convert TCP packet traces files into text and pcap readable formats:

```
RP/0/RP0/CPU0:ios# tcp dump-file convert all-formats all
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_53.462070.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_40.154838.pcap
[OK]
```

The following example shows how to filter TCP dump packet traces by IP address and convert them into text and pcap readable format:

```
RP/0/RP0/CPU0:ios# tcp dump-file convert all-formats ipaddress 192.0.2.121
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_1_1_1_2_node0_RSP0_CPU0_2024_3_19_10_9_20.539021.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_1_1_1_2_node0_RSP0_CPU0_2024_3_19_10_9_20.539021.pcap
[OK]
```

The following example specifies a location where you want to store the converted TCP dump file:

```
RP/0/RP0/CPU0:ios# tcp dump-file convert all-formats all location 0/RP0/CPU0
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_12_53_35.12323.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_12_53_35.12323.pcap
[OK]
```

The following example specifies the absolute file path where you want to store the converted TCP dump files:

```
RP/0/RP0/CPU0:ios# tcp dump-file convert text all file /harddisk:/demo2
ascii file is saved at : /harddisk:/demo2.txt
[OK]
```

tunnel-id

To specify the ID of the GMPLS UNI tunnel, use the **tunnel-id** command in GMPLS UNI controller tunnel-properties configuration sub-mode.

tunnel-id *number*

Syntax Description

number	Specifies the tunnel ID.

Command Default

None

Command Modes

GMPLS UNI controller tunnel-properties configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to specify a tunnel ID.

```
RP/0/RP0/CPU0:ios(config)#mpls traffic-eng
RP/0/RP0/CPU0:ios(config-mpls-te)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-te-gmpls)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-te-gmpls-cntl)#tunnel-properties
RP/0/RP0/CPU0:ios(config-te-gmpls-tun)#tunnel-id 5
RP/0/RP0/CPU0:ios(config-te-gmpls-tun)#
```

tunnel-properties

To configure tunnel-specific information for a GMPLS UNI controller, use the **tunnel-properties** command in GMPLS-UNI configuration sub-mode.

tunnel-properties

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

GMPLS UNI configuration

Command History

Release	Modification
Release 7.0.1	This command is introduced.

Example

The following example shows how to enter the sub-mode to configure tunnel-specific information for a GMPLS UNI controller.

```
RP/0/RP0/CPU0:ios(config)#mpls traffic-eng
RP/0/RP0/CPU0:ios(config-mpls-te)#gmpls optical-uni
RP/0/RP0/CPU0:ios(config-te-gmpls)#controller Optics0/0/0/0
RP/0/RP0/CPU0:ios(config-te-gmpls-cntl)#tunnel-properties
RP/0/RP0/CPU0:ios(config-te-gmpls-tun)#
```

working-controller

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

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

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

Syntax Description

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

Command Default

None

Command Modes

Configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Example

This example shows how to configure an ODU4 controller as the working controller in the ODU group 2 controller:

```
RP/0/RP0:hostname(config)# controller Odu-Group-Mp 2 signal Otn odu-type ODUC4
RP/0/RP0:hostname(config-odu-group-mp 1)# working-controller ODUC4 0/0/0/12
```