# Configuring Controllers

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

Optics Controllers

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

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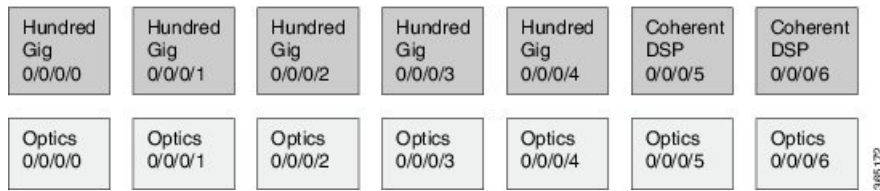
Maintenance Mode

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

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

Configure Optics Controller

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

configure

controller *controllertype Rack/Slot/Instance/Port*

rx-high-threshold *rx-high*

tx-high-threshold *tx-high*

cd-max *cd-max*

cd-min *cd-min*

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

commit

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

Example

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

```
configure
controller optics 0/0/0/1
rx-high-threshold 200
tx-high-threshold 300
```

```
cd-max 10000
cd-min 2000
dwdm-carrier 50GHz-grid wavelength 1560200
commit
```

Associated Commands

- controller optics

- show controllers

Configure Wavelength

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

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

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

To configure wavelength, use the following commands.

configure

controller optics *Rack/Slot/Instance/Port*

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

commit

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

Example

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

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

Associated Commands

- dwdm-carrier

- show controllers

Breakout Mode

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

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

The client ports can operate at 10G mode using the breakout cable or the breakout patch panel. All five client ports of the slice need to be configured at the same bitrate. The controllers are represented in the *Rack/Slot/Instance/Port/Lanenumber* format; for example, 0/0/0/1/3. The range of *Lanenumber* is from 1 to 4.

Four TenGig Ethernet controllers are created for each client port in breakout mode. The following figure describes the controller representation when the client rate is 10G and the trunk rate is 100G.
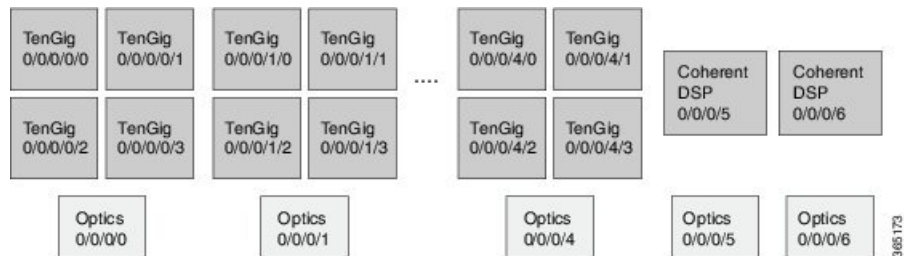
When the optics controller is shutdown, all four TenGig Ethernet controllers are shut down. Individual 10G port can be turned off from the TenGig Ethernet controller.

Laser Squelching

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

Configure IDLE Insertion

When a fault occurs on the trunk port, the user can hold the propagation of Local Fault using the IDLE insertion feature. This feature can be used on customer deployments to prevent reset of client ports during a PSM switchover.

Enabling IDLE hold off timer in 100GE Controllers

This feature must be enabled for each 100GE client port. Only port based configuration is supported.

You can enable the IDLE insertion feature by using the following commands:

RP/0/RP0/CPU0:ios(config)#controller hundredGigECtrlr *Rack/Slot/Instance/Port*

RP/0/RP0/CPU0:ios (config-eth-ctrlr)# holdoff-time trunk-fault *timevalue*

The following is an example for enabling IDLE hold off timer in 100GE Controllers:

Example

```
RP/0/RP0/CPU0:ios(config)#controller hundredGigECtrlr 0/0/0/4
RP/0/RP0/CPU0:ios (config-eth-ctrlr)# holdoff-time trunk-fault timevalue
                    <timevalue : in milliseconds>
RP/0/RP0/CPU0:ios(config-eth-ctrlr)#holdoff-time trunk-fault 3000
```

The range of *timevalue* is 10 ms to 3 sec.

When the fault occurs on the trunk for the duration of configured timevalue, idles are inserted in traffic stream from trunk port to client port.

When the trunk port remains faulty beyond the configured *timevalue*, Local Fault is transmitted towards client device.

When the trunk recovers from the fault before the timevalue expires, the traffic resumes.

Note This feature is supported on 100GE client ports in NCS 1002 slice mode, mixed mode slice client, and MACsec modes.

Limitations

The timer functionality is implemented in software. Hence, Local Fault propagation after the timeout do not resume during headless event.

When the feature is configured, Local Faults (including far-end client) are suppressed and the idles are inserted. This results in the laser-squelch not being supported.

Viewing the hold off timer

You can view the hold off timer configured over 100GE client interfaces using the following command:

RP/0/RP0/CPU0:ios#show controllers hundredGigECtrlr *Rack/Slot/Instance/Port*

Example

```
RP/0/RP0/CPU0:ios#show controllers hundredGigECtrlr 0/0/0/4
Mon Jun 11 21:14:37.612 IST
Operational data for interface HundredGigECtrlr0/0/0/4:

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: Disabled

Phy:
    Media type: Not known

Autonegotiation disabled.

Operational values:
    Speed: 100Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    BER monitoring:
```

```
        Not supported
    Holdoff Time: 3000ms
```

Unconfiguring Hold Off timer in 100GE Controllers

You can unconfigure the Hold Off timer over 100GE client interfaces using the following command

```
RP/0/RP0/CPU0:ios#conf t
Mon Jun 11 21:11:49.482 IST
RP/0/RP0/CPU0:ios(config)#controller hundredGigECtrlr 0/0/0/4
RP/0/RP0/CPU0:ios(config-eth-ctrlr)#no holdoff-time trunk-fault 3000
RP/0/RP0/CPU0:ios(config-eth-ctrlr)#commit
```

After unconfiguring the holdoff-timer, the output of show controllers command is as follows

```
RP/0/RP0/CPU0:ios#show controllers hundredGigECtrlr 0/0/0/4
Mon Jun 11 21:14:37.612 IST
Operational data for interface HundredGigECtrlr0/0/0/4:

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: Disabled

Phy:
    Media type: Not known

Autonegotiation disabled.

Operational values:
    Speed: 100Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: None (or external)
    BER monitoring:
        Not supported
    Holdoff Time: 0ms
```

Note Hold off timer at Ethernet controller is supported only at 100GE client ports and NOT supported at 10GE, 40GE client interfaces, but if enabled the port is blocked in the configuration mode

```
RP/0/RP0/CPU0:ios(config)#controller tenGigECtrlr 0/0/0/3/1
RP/0/RP0/CPU0:ios(config-eth-ctrlr)#holdoff-time trunk-fault ?
  <0-3000>  Time in ms
RP/0/RP0/CPU0:ios(config-eth-ctrlr)#holdoff-time trunk-fault 3000
RP/0/RP0/CPU0:ios(config-eth-ctrlr)#commit
Tue Jun 12 02:39:21.641 IST


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

LLDP Snooping

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

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

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

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

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

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

        LLDP Neighbor Snoop Data
------------------------------------------------
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Local Controller:     HundredGigECtrlr0/0/0/8

Source MAC Address:   0010.9400.0002

Chassis ID:           ABCD

Port ID:              192.0.2.254

Port Description:     descr:ABCD Port-iter2

System Name:          Name:ABCD

System Description:   descr:ABCD-iter2

Hold Time(TTL):       120 seconds

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

Enabled Capabilities: P,R,T

Management Address:
        IPv4 address: 192.0.2.254
```

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

```
RP/0/RP0/CPU0:ios# show lldp neighbors
Thu Jul 26 15:08:27.943 IST
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
```

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

Device ID          Local Intf         Hold-time  Capability      Port ID
Hav                EC0/0/0/4          120         B,R              Ethernet1/1

Total entries displayed: 1
```

EC refers to Ethernet Controller.

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

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

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

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

Time remaining: 103 seconds
Hold Time: 120 seconds
System Capabilities: B,R
Enabled Capabilities: B,R
Management Addresses:
  IPv4 address: 10.77.132.26

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


Total entries displayed: 1
```

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

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

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

```
RP/0/RP0/CPU0:ios# show lldp neighbors
Fri Feb  3 13:21:09.779 IST
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID        Local Intf       Hold-time  Capability      Port ID
Spirent Test Center2 EC0/0/0/11/1        60          R,S             0194.3333.3333
Spirent Test Center2 EC0/0/0/11/2        60          R,S             0194.5555.5555
Spirent Test Center2 EC0/0/0/11/3        60          R,S             0194.2020.2121
Spirent Test Center2 EC0/0/0/11/4        60          R,S             0194.8888.8888
ROSCO NCS1K EC0/0/0/25/2                 60          P,R,S           0194.4444.4444
Spirent Test Center2 EC0/0/0/25/2        60          R,S             0194.6666.6666
Spirent Test Center2 EC0/0/0/25/3        27          R,S             0194.0000.0001
Spirent Test Center2 EC0/0/0/25/4        60          R,S             0194.0000.0011
```

LLDP Snoop and Drop

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

Limitation:

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

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

Prerequisites:

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

Configuring Slices and LLDP Drop at Slice Level

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

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

configure

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

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

commit

Example:

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

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

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

configure

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

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

commit

Example:

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

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

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

Associated Commands

- hwmodule
- show controllers

Verifying the Status of LLDP Drop

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

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

Example:

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

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

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

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

Example :

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

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

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

Disabling LLDP Drop

To disable LLDP drop, use the following commands.

configure

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

commit

Example:

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

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

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

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

Configure Ethernet Controller

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

configure

controller *controllertype Rack/Slot/Instance/Port*

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

sec-admin-state *admin-state*

laser-squelch

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

commit

Example

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

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

Associated Commands

- controller GigECtrlr
- show controllers

Configure the Coherent DSP Controller

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

configure

controller *controllertype Rack/Slot/Instance/Port*

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

sec-admin-state *admin-state*

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

commit

Example

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

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

Associated Commands

- controller coherentDSP

- show controllers

Configure Loopback

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

configure

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

commit

Example

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

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

Associated Commands

- controller optics

- controller GigECtrlr

- controller coherentDSP

Restore Factory Settings

You can restore factory settings. The **commit replace** command replaces the entire running configuration with the contents of the target configuration. If the target configuration is empty, all existing configurations

are removed and NCS 1002 will be restored to factory configuration. To restore NCS 1002 to factory settings, use the following commands.

configure

commit replace

Example

```
configure
commit replace
```

Headless Mode

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

View the Headless Statistics

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

Procedure

---

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

Example:
```
RP/0/RP0/CPU0:ios# show controllers hundredGigECtrlr 0/0/0/11 headless-stats
```
Displays the statistics collected during the last headless operation. The collected statistics is preserved for a slice until the hw-module configuration is removed or changed on that slice or until the next headless operation. The statistics is also preserved across process restarts.

Associated Commands

- show controllers

Configure IP Accesss List

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

configure

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

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

commit

Example

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

Sample Configuration for IPv4 Access Lists

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

Sample Configuration for IPv6 Access Lists

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

Verify IPv6 ACL

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

Examples to check statistics

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

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

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

```
Wed Jan 17 09:52:14.591 IST
ipv6 access-list IPV6_ROUTER_FWD_TELNET_TRAFFIC_DENY
10 deny tcp any any eq telnet (3 matches)
20 permit ipv6 any any (5 matches)
ipv6 access-list IPV6_SSH_DENY
10 deny tcp any any eq ssh (9 matches)
```

```
20 permit ipv6 any any (100 matches)
RP/0/RP0/CPU0:PROD_20#
```