OLT Network Configuration

- arp , on page 3
- arp aging-time, on page 4
- description *interface-name*, on page 5
- dhcp-snooping , on page 6
- dhcp-snooping trust , on page 7
- dlf forward, on page 8
- interface, on page 9
- interface loopback-interface, on page 11
- interface vlan-interface, on page 12
- ip-source-guard, on page 13
- ip-source-guard filter, on page 14
- ip address, on page 15
- ip address *mask-ip-address*, on page 16
- ip address range, on page 17
- ip icmp mask-reply, on page 18
- ip icmp unreachable, on page 19
- mac-address-table, on page 20
- mac-address-table learning, on page 21
- mac-address-table age-time, on page 22
- mac-address-table blackhole, on page 23
- mac-address-table max-mac-count, on page 24
- mirror destination-interface, on page 25
- mirror source-interface, on page 26
- show arp, on page 27
- show dhcp-snooping clients, on page 28
- show dhcp-snooping interface, on page 29
- show dlf-forward, on page 31
- show ip interface, on page 32
- show ip source guard, on page 33
- show mac-address-table age-time, on page 34
- show mac-address-table, on page 35
- show mirror, on page 37
- show snmp community, on page 38

- show snmp contact, on page 39
- show snmp engineid, on page 40
- show snmp group, on page 41
- show snmp host, on page 42
- show snmp location, on page 43
- show snmp mib, on page 44
- show snmp name, on page 45
- show snmp notify, on page 46
- show snmp user, on page 47
- show snmp view, on page 48
- shutdown, on page 49
- snmp-server, on page 50
- snmp-server community, on page 51
- snmp-server community encrypt, on page 52
- snmp-server contact, on page 53
- snmp-server encrypt, on page 54
- snmp-server engineid, on page 55
- snmp-server group, on page 56
- snmp-server host, on page 57
- snmp-server location, on page 59
- snmp-server max-packet-length, on page 60
- snmp-server name, on page 61
- snmp-server trap-source, on page 62
- snmp-server user, on page 63
- snmp-server view, on page 65

arp

To add a static entry in the Address Resolution Protocol (ARP) table, use the **arp** command in the global configuration mode. To remove an entry from the ARP table, use the **no** form of the command.

[**no**] **arp***ip-address* **mac***mac-address* [**vid** *vlan-id* | **port** *port-id*]

Syntax Description

ip-address	IPv4 address for which a permanent entry is added to the ARP table. Enter the IPv4 address in a four-part dotted-decimal format that corresponds to the local data-link address (a 32-bit address)
mac *mac-address*	Hardware MAC address that the IPv4 address is linked to. Enter the MAC address in dotted-hexadecimal notation.
vid *vlan-id*	(Optional) Specifies the configured VLAN.
port *port-id*	(Optional) Specifies the configured port

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

You can manually configure and maintain a static ARP entry. It cannot be aged or overwritten by dynamic ARP entry. A static ARP entry can be a long or a short entry. A static ARP entry comprises IP address and the corresponding MAC address. A long static ARP entry comprises the VLAN and egress interface details along with the IP address and MAC address. Long Static ARP entries can be directly used for packet forwarding.

When you manually configure a Long Static ARP entry, the IP address in the entry must be in the same network segment as the IP address of the VLAN interface on which the egress interface resides.

A short static ARP entry comprises the IP Address and the MAC Address. A short static ARP entry cannot be directly used for packet forwarding. A shorts static ARP request packet is sent by the host. If the source IP address and the source MAC address in the received response packet are the same as the configured IP address and MAC address, the ARP entry will be completed. Then it can be used for packet forwarding.

Example

This example shows how to configure a short static ARP entry:

```
Device> enable
Device# configure terminal
Device(config)# arp 192.168.1.19 mac 00:02:9a:3b:94:d9
```

arp aging-time

To specify how long an entry can exist in an ARP table, use the **arp aging-time** command in the global configuration mode.

arp aging-time *aging-time*

Syntax Description

aging-time	Specify the timeout period in seconds.

Command Default

The default timeout of an ARP table entry is 20 minutes.

Command Modes

Global configuration (config)

Example

This example shows how to configure the aging time for ARP table entries:

```
Device> enable
Device# configure terminal
Device(config)# arp aging-time 300
```

description *interface-name*

To configure the interface description, use the **description** *interface name* in the VLAN configuration mode. You can delete the interface description by using the**no** form of the command.

description *interface-name*

no description *interface-name*

Syntax Description

interface-name	Adds a description for the interface.

Command Default

None

Command Modes

VLAN configuration

Examples

The following example shows how to configure the IP interface description

```
Device(config-if-vlanif)# description interface1
```

dhcp-snooping

To enable Dynamic Host Control Protocol (DHCP) snooping feature on a device, use the **dhcp-snooping** command in the global configuration mode.

dhcp-snooping [**port-down-action fast-remove**]

Syntax Description

port-down-action fast-remove	Configures the link down operation on the port.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

When DHCP Snooping is enabled on your device, it monitors and validates the DHCP packets that it receives. Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets that are received from DHCP servers. Trusted ports forward the received DHCP packets to DHCP clients.

To configure DHCP Snooping feature, use the **dhcp-snooping** command.

When a link in the network goes down, use the **dhcp-snooping port-down-action fast remove** command to remove the corresponding entry from the DHCP binding database.

Example

This example shows how to configure DHCP Snooping on a device:

```
Device> enable
Device# configure terminal
Device(config)# dhcp-snooping
```

dhcp-snooping trust

To configure an interface as trusted for Dynamic Host Control Protocol (DHCP) snooping operations, use the **dhcp-snooping trust** command in the interface configuration mode.

dhcp-snooping trust

Command Default None

Command Modes Global configuration (config)

Example

This example shows how to configure a trusted interface for DHCP Snooping:

```
Device> enable
Device# configure terminal
Device(config)# interface g0/1
Device(config-if)# dhcp-snooping trust
```

dlf forward

To enable the forwarding of Destination Lookup Failure (DLF) unicast or multicast packets, use the **dlf forward** command. To enable DLF forwarding on egress packets of all ports, use the command in the global configuration mode. To enable DLF forwarding on the egress packets of a specific port, use the command in the interface configuration mode. DLF Forwarding is disabled by default. To disable it use the **no** form of the command.

dlf-forward { **unicast** | **multicast** }

no dlf-forward { **unicast** | **multicast** }

Syntax Description

unicast	Enables the forwarding function of DLF unicast packets
multicast	Enables the forwarding function of DLF multicast packets

Command Default

DLF forwarding is disabled by default.

Command Modes

Global configuration mode.
Interface configuration mode.

Examples

The following example shows how to configure DLF forwarding for unicast packets for all egress ports:

```
Device(config)# dlf-forward unicast
```

The following example shows how to configure DLF forwarding for unicast packets on a specific port:

```
Device(config)# interface ethernet 1/4
       Device(config-if)# dlf-forward unicast
```

The following example shows how to configure DLF forwarding for multicast packets for all egress ports:

```
Device(config)# dlf-forward multicast
```

The following example shows how to configure DLF forwarding for multicast packets on a specific port:

```
Device(config)# interface ethernet 1/4
       Device(config-if)# dlf-forward multicast
```

interface

To configure an interface and enter into Interface configuration mode, use the **interface** command in the global configuration mode.

interface {*port-id* | **ethernet** *slot-num/port-num* | **gpon** *slot-num/port-num* | **loopback-interface** *loopback-int-number* | **meth-interface** *meth-int-number* | **range** {**ethernet** *port-num/slot-num* | **gpon** *port-num/slot-num* } | **vlan-interface** *vlan-id* }

Syntax Description

port-id	Specifies the port to be configured. It is a string consisting of 4 to 14 characters.
ethernet *slot-num/port-num*	Enables you to configure Ethernet ports. For a Gigabit Ethernet port, *slot-num* is 1 and *port-num* ranges from 1 through 4. For a Ten Gigabit Ethernet port, *slot-num* is 2 and *port-num* ranges from 1 through 2.
gpon *slot-num/port-num*	Enables you to configure GPON ports. *slot-num* is 0 and *port-num* ranges from 1 through 8.
loopback-interface *loopback-int-number*	Enables you to configure a loopback interface. *loopback-int-number* number can be 0 or 1.
meth-interface *meth-int-number*	Enables you to configure the Management Interface, MEth, that allows you to log in and perform configurations.
range {**ethernet** *port-num/slot-num* | **gpon** *port-num/slot-num* }	Enables you to configure a range of ethernet interfaces or a range of GPON interfaces.
vlan-interface *vlan-id*	Enables you to configure a VLAN interface. *vlan-id* specifies the VLAN id. Values range from 1 through 4094.

Command Modes

Global Configuration (config)

Command Default

None

Usage Guidelines

Use the **interface** command to enter the Interface Configuration mode and configure the interface.

To configure a range of interfaces at once, use the **interface range** command. In the interface range configuration mode, all entered commands are applicable to all interfaces within that range.

Example

The following example configures an Ethernet interface:

```
Device#configure terminal
Device(config)#interface ethernet 1/1
Device(config-if-ethernet-1/1)#
```

The following example configures a range of GPON interfaces:

```
Device#configure terminal
Device(config)#interface range gpon 0/1 to gpon 0/3
```

interface loopback-interface

To create a loopback interface and to enter the loopback interface configuration mode, use the **interface loopback-interface** command in the Global configuration mode.

To disable a loopback interface use the **no** form of the command.

interface loopback-interface *interface-number*

no interface loopback-interface

Syntax Description

loopback-interface	Configures a loopback interface.
interface-number	Configures the loopback interface number.

Command Default

None

Command Modes

Global configuration mode

Examples

The following example shows how to configure a loopback interface:

```
Device(config)# interface loopback-interface 1
```

interface vlan-interface

To create a VLAN interface and enter interface configuration mode, use the **interface vlan-interface** command in the global configuration mode. To remove a VLAN interface, use the **no** form of the command.

interfacevlan-interface *vlan-id*

no interfacevlan-interface

Syntax Description

vlan-id	Sets the VLAN for the interface. The range is from 1-4094.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure an interface VLAN:

```
Device(config)# interface vlan-interface 1
```

ip-source-guard

To enable IP Source Guard feature on a device, use the **ip-source-guard** command in the global configuration mode.

ip-source-guard { **vlan** *vlan-list* | **permit igmp** | **bind ip** *ip-address* [**mac** *mac-address* **interface** { **ethernet** | **gpon** } *interface-id* **vlan** *vlan-id*] }

Syntax Description

vlan *vlan-list*	Configures IP Source Guard on the VLANs listed by *vlan-list*.
permit igmp	Configures IP Source Guard to allow Internet Group Management Protocol (IGMP) packets to pass through.
bind ip *ip-address*	Configures an entry in the static IP source binding table.
mac *mac-address*	The MAC address that is bound to the IP address.
interface	Specifies the interface to be configured.
ethernet	Specifies the Ethernet interface
gpon	Specifies the GPON interface
vlan *vlan-id*	Specifies the VLAN to which the interface belongs.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

IP Source Guard feature filters the source IP address on a Layer 2 port to prevent a malicious host from impersonating a legitimate host.

You can enable the IP Source Guard feature only on untrusted ports. For IP Source Guard to function, enable DHCP Snooping.

Use the **ip-source-guard bind** command to configure an IP source binding.

Use the **ip-source-guard vlan** *vlan-list* command to configure IP Source Guard on the listed VLANs.

Use the **ip-source-guard permit igmp** command to allow IGMP packets to pass through.

Example

The following example shows how to configure an entry in the IP source binding table:

```
Device> enable
Device# configure terminal
Device(config)# ip-source-guard bind ip 192.168.11.2
```

The following example shows how to configure ip source guard on three VLANs:

```
Device(config)# ip-source-guard vlan 7,8,10
```

ip-source-guard filter

To configure the port filtering mode for an interface, use the **ip-source-guard** command in the interface configuration mode.

```
ip-source-guard [ip |ip-mac | ip-mac-vlan]
```

Syntax Description

ip	Specifies that the port filter packets are based on source IP, regardless of the MAC address and the VLAN ID.
ip-mac	Specifies that the port filters packets based on the source IP address and the MAC address of the packet.
ip-mac-vlan	Specifies that the port filters packets based on source IP address, MAC address, and VLAN ID.

Command Default

None

Command Modes

Interface Configuration (config-if)

Usage Guidelines

IP Source Guard feature filters the source IP address on a Layer 2 port to prevent a malicious host from impersonating a legitimate host.

You can enable the IP Source Guard feature only on untrusted ports. For IP Source Guard to function, enable DHCP Snooping.

Use the **ip-source-guard ip** command on the interface to filter packets are based on source IP, regardless of the MAC address and the VLAN ID.

Use the **ip-source-guard ip-mac** *vlan-list* command on the interface to filter packets are based on source IP and MAC address, regardless of the VLAN ID.

Use the **ip-source-guard ip-mac-vlan** command on the interface to filter packets are based on source IP, MAC address,and VLAN ID.

If you don't specify the port filtering mode, the port filters packets based on the source IP address, MAC address, and VLAN ID.

Example

The following example shows how to configure the port to filter packets based on the source IP address and MAC address:

```
Device> enable
Device# configure terminal
Device(config)# interface etherent 1/1

Device(config-if-ethernet-1/1)# ip-source-guard ip-mac
Config IP source guard mode of port successfully.
```

ip address

To configure the primary IP address for the VLAN interface, use the **ip address** command in the VLAN configuration mode.

ip address { *ip-addressmask-ip-address***override** | **primary** *ip-address* }

Syntax Description

Override	Overrides the IP address of the VLAN interface.
primary	Configures the primary IP address for the VLAN interface.

Command Default

None

Command Modes

VLAN configuration

Examples

The following example shows how to configure the pimary IP address for an interface:

```
Device(config-if-vlan)# ip address primary 192.0.2.1
```

ip address *mask-ip-address*

To configure a loopback interface for the IP address, use the **ip address** *mask-ip-address* command in the loopback interface configuration mode.

To disable the loopback loopback interface for the IP address, use the **no** form of the command.

ip address*ip-address mask-ip-address*

no ip address*ip-address mask-ip-address*

Syntax Description

ip-address	It is the IP address of the interface
mask-ip-address	Configures the loopback IP address for the interface.

Command Default

None

Command Modes

Loopback interface configuration mode

Examples

The following example shows how to configure a loopback interface for the IP address

```
Device(config-if-loopbackinterface)# ip address 192.0.2.1 255.255.255.0
```

ip address range

To configure the range of IP addresses for the VLAN interface, use the **ip address range** command in the the VLAN configuration mode. You can delete the range of IP addresses for the VLAN interface using the **no** form of the command.

ip address range { *start-ip-address end-ip-address* }

no ip address range { *start-ip-address end-ip-address* }

Syntax Description

range	Configures the range of IP addresses for the VLAN interface
start-ip-address	Configures the starting IP address of the range.
end-ip-address	Configures the ending IP address of the range.

Command Default

None

Command Modes

VLAN configuration mode

Examples

The following example shows how to configure a range of IP addresses for the interface:

```
Device(config-if-vlan)# ip address range 192.0.2.254 192.0.2.255
```

ip icmp mask-reply

To enable the ICMP address mask reply packet, use the **ip icmp mask-reply** command in the global configuration mode. To disable the ICMP address mask reply packet, use the **no** form of the command.

ip icmp mask-reply

no ip icmp mask-reply

Syntax Description

mask-reply	Enables the ICMP address mask reply packet.

Command Default

None

Command Modes

Global configuration mode

Examples

The following example shows how to enable ICMP address mask reply packet:

```
Device(config)# ip icmp mask-reply
```

ip icmp unreachable

To enable the sending of ICMP destination unreachable packets, use the **ip icmp unreachable** command in the VLAN configuration mode. To disable the sending of ICMP destination unreachable packets, use the **no** form of the command.

ip icmp unreachable

no ip icmp unreachable

Syntax Description

unreachable	Enables the sending of ICMP destination unreachable packets.

Command Default

None

Command Modes

VLAN configuration mode

Examples

The following example shows how to enable the sending of ICMP destination unreachable packets.

```
Device(conifg-if-vlanif)# ip icmp unreacheable
```

mac-address-table

To add a MAC address manually to the MAC address table, use the **mac-address-table** command in the global configuration mode. To remove a MAC address from the table, use the **no** form of the command.

mac-address-table {**static** | **permanent** | **dynamic**} *mac-address* **interface ethernet***interface-number* **vlan** *vlan-id*

no mac-address-table {**static** | **permanent** | **dynamic**} *mac-address* **interface ethernet***interface-number* **vlan** *vlan-id*

Syntax Description

static	Adds a static MAC address to the MAC address table.
permanent	Adds a MAC address permanently to the MAC address table.
dynamic	Adds a dynamic MAC address to the MAC address table.

Command Default

None

Command Modes

Global configuration

Examples

The following examples shows how to add a static MAC address to a MAC address table:

```
Device(config)# mac-address-table static 00:50:3e:8d:64:00 interface ethernet
 1/4 vlan 3
```

mac-address-table learning

To disable dynamic MAC address learning, use the **no mac-address-table learning** command. To disable MAC address learning on all ports use the command in the global configuration mode. To disable MAC address learning on specific ports use the command in the interface configuration mode. MAC address learning is enabled by default.

mac-address-table learning

no mac-address-table learning

Syntax Description

learning	Enables or disables MAC address learning.

Command Default

MAC address learning is enabled by default.

Command Modes

Global configration
Interface configuration

Examples

The folowing example shows how to disable MAC address learning on an ethernet port:

```
Device(config)# interface ethernet 1/4
Device(config-if-ethernet-1/4)# no mac-address-table learning
```

mac-address-table age-time

To configure the aging time for entries in the MAC address table, use the **mac-address-table age-time** command in the global configuration mode. To disable the aging process use the **disable** keyword.

mac-address-table age-time {*seconds* | **disable**}

Syntax Description

disable	Disables the ageing process for the MAC address table.
seconds	Configures the ageing time for the MAC address table in seconds.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to configure ageing time for a MAC address table:

```
Device(config)# mac-address-table age-time 120
```

mac-address-table blackhole

To add the MAC address of an untrusted user as a Blackhole MAC address, use the **mac-address-table blackhole** command in the global configuration mode. To remove a MAC addeess as a Blackhole MAC address use the **no** form of the command.

mac-address-tableblackhole *mac-address* **vlan** *vlan-id*

no mac-address-tableblackhole *mac-address* **vlan** *vlan-id*

Syntax Description

blackhole	Adds a MAC address as a Blackhole MAC address.

Command Default

None

Command Modes

Global configuration

Examples

The following example shows how to add a MAC address as a Blackhole MAC address:

```
Device(config)# mac-address-table blackhole 00:05:00:05:00:05 vlan 1
```

mac-address-table max-mac-count

To configure the maximum number of MAC addresses that will be learnt by the MAC Address Table on a port, use the **mac-address-table max-mac-count** command in the interface configuration mode. To keep the number of MAC addresses learnt as unlimited use the **no** form of the command. By default, the number of MAC addresses that are dynamically learnt by the MAC Address Table are unlimited.

mac-address-table max-mac-count *integer*

no mac-address-table max-mac-count *integer*

Syntax Description

max-mac-count *integer*	Enables a limit on the number of dynamically learnt MAC addresses added to the table

Command Default

The number of learnt MAC addresses are unlimited by default

Command Modes

Interface configuration

Examples

The following example shows how to enable a maximum learnt MAC address count on a port:

```
Device(config)# interface ethernet 1/4
Device(config-if-ethernet-1/4)# mac-address-table max-mac-count 500
```

mirror destination-interface

To configure a port as destination port for mirroring, use the mirror destination-interface command in the global configuration mode. To remove the mirroring configuration, use the **no** form of the command.

[**no**] **mirror destination-interface** {**ethernet** *slot/port* | **gpon** *slot/port*}

Syntax Description

ethernet *slot/port*	Specifies the ethernet interface that can be configured as the destination for port mirroring
gpon *slot/port*	Specifies the GPON interface as the destination for port mirroring.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to configure the destination port that receives the mirrored packets.

Port mirroring duplicates the data packets on the monitored (source) port and sends the packets to a destination port for monitoring or analysis. You can mirror inbound packets or outbound packets or both types of packets on the source port.

A port configured as a destination port cannot be used as a normal port.

For a switch, you can configure only one port as destination port.

Example

The following example sets the ethernet port 2/1 as the destination for mirroring.

```
Device#configure terminal
Device(config)#mirror source-interface ethernet 1/1 both

Device(config)#mirror destination-interface ethernet 2/1
```

mirror source-interface

To configure a port to act as a source port for mirroring, use the **mirror source-interface** command in the global configuration mode. To remove the mirroring configuration, use the **no** form of the command.

[**no**] **mirror source-interface** {**ethernet** *slot/port* | **cpu** | **gpon** *slot/port* }{**ingress** | **egress** | **both**}

Syntax Description

ethernet *slot/port*	Specifies the ethernet interface that can be configured as the source for port mirroring
cpu	Specifies the CPU as the source for port mirroring
gpon *slot/port*	Specifies the GPON interface as the source for port mirroring.
ingress	Specifies that the packets at the ingress of the specified port, which are inbound, are mirrored.
egress	Specifies that packets at the egress of the specified port, which are outbound, are mirrored.
both	Specifies that the packets at both the ingress and egress interfaces are mirrored.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to configure the source port for mirroring the packets at the port. You can mirror inbound packets or outbound packets or both types of packets.

Port mirroring duplicates the data packets on the monitored (source) port and sends the packets to a destination port for monitoring or analysis.

You can configure multiple ports as source port for mirroring.

Example

The following example sets the ethernet port 1/1 as the source for mirroring the packets.

```
Device#configure terminal
Device(config)#mirror source-interface ethernet 1/1 both
```

show arp

To display the Address Resolution Protocol (ARP) table entries, use the **show arp** command in privileged or global configuration mode.

show arp {**dynamic** | **static** | **all** }

Syntax Description

dynamic	Displays all the dynamic ARP table entries
static	Displays all the static ARP table entries
all	Displays all the entries from the ARP table

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

The **show arp dynamic** command displays all mappings and information about each entry in the ARP table, including the aging time, VLAN instance, and port.

Example

```
Device#show arp dynamic
Informations of ARP
d - days, h - hours, m - minutes, s - seconds
IpAddress       Mac_Address        Vlan  Port     VPTag Type     ExpireTime   Status
10.75.171.1     00:23:5d:fd:94:00  100   e1/3     0     dynamic  18m34s       valid
10.75.171.71    00:50:56:92:1d:fb  100   e1/3     0     dynamic  10m51s       valid
10.75.171.79    00:0c:29:80:8b:59  100   e1/3     0     dynamic  17m43s       valid
10.75.171.91    00:0c:29:71:b1:4f  100   e1/3     0     dynamic  10m59s       valid
10.75.171.138   00:0c:29:f9:35:c3  100   e1/3     0     dynamic  11m07s       valid

Total entries:5
```

Table 1: Description of the show arp dynamic Command Output

IPAddress	Specifies the IP address of the ARP table entry
MAC_Address	Specifies the MAC address associated with the IP address
Vlan	Specifies the VLAN to which this interface belongs
Port	Specifies the port that has learnt the ARP entry
VPTag	Specifies the virtual port for GPON routing
Type	Specifies whether it is a dynamic or a static entry
Expire Time	Displays the time remaining before the ARP entry expires
Status	Specifies whether the entry is valid or not.

show dhcp-snooping clients

To display binding between the IP address and the MAC address that is recorded by DHCP Snooping, use the **show dhcp-snooping clients** command in privileged or global configuration mode.

```
show snmp dhcp-snooping clients
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

The following example shows a sample format of the output of this command:

```
Device#show dhcp-snooping clients
DHCP client information:
d - days, h - hours, m - minutes, s - seconds
IPAddress        mac               vlan  port     LeaseTime      ExceedTime

Total entries: 0. Printed entries: 0.
```

Related Commands

Command	Description
dhcp-snooping	Enables DHCP Snooping on the device.

show dhcp-snooping interface

To display the details of DHCP Snooping on an interface, use the **show dhcp-snoopign interface** command in privileged or global configuration mode.

```
show dhcp-snooping interace [ethernet | gpon][interface-id]
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

This command displays the DHCP Snooping enabled state, information on the trusted port, the number of DHCP clients allowed on the physical port, and the number of currently connected DHCP clients.

Example

```
Device#show dhcp-snooping interface
Config information of DHCP Snooping:
DHCP Snooping status:Enable
DHCP Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
g0/1          untrust   2048          0             0
g0/2          untrust   2048          0             0
g0/3          untrust   2048          0             0
g0/4          untrust   2048          0             0
g0/5          untrust   2048          0             0
g0/6          untrust   2048          0             0
g0/7          untrust   2048          0             0
g0/8          untrust   2048          0             0
e1/1          untrust   2048          0             0
e1/2          untrust   2048          0             0
e1/3          untrust   2048          0             0
e1/4          untrust   2048          0             0
e2/1          untrust   2048          0             0
e2/2          untrust   2048          0             0


Device#show dhcp-snooping interface gpon 0/1

Config information of DHCP Snooping:
DHCP Snooping status:Enable
DHCP Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
g0/1          untrust   2048          0             0


Device#show dhcp-snooping interface ethernet 1/1

Config information of DHCP Snooping:
DHCP Snooping status:Enable
DHCP Snooping port-down-action fast-remove:Enable
Port information:
Port          mode      maxclients    clients(ack)  clients(unack)
```

```
e1/1            untrust   2048          0              0
```

show dlf-forward

To display the DLF forwarding configuration for a port, use the **show dlf-forward** command in the EXEC mode.

show dlf-forward interface { **ethernet** *port-number* | **gpon** *port-number* }

Syntax Description

ethernet *port-number*	Displays the DLF Forwarding configuration for the ethernet port.
gpon *port-number*	Displays the DLF Forwarding configuration for the gpon port.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The following example shows how to display the DLF forwarding configuration for an ethernet port

```
Device# show dlf-forward interface ethernet 1/1
Forwarding unknown unicast packets global status:  disable
Forwarding unknown multicast packets global status:  disable
Port      Forwarding Unknown Unicast      Forwarding Unknown Multicast
e1/1      disable                         disable
```

Examples

The following example shows how to display the DLF forwarding configuration for a GPON port

```
Device# show dlf-forward interface gpon 0/1
Forwarding unknown unicast packets global status:  disable
Forwarding unknown multicast packets global status:  disable
Port      Forwarding Unknown Unicast      Forwarding Unknown Multicast
g0/1      disable                         disable
```

show ip interface

To display the IP interface configuration for the Layer 3 device, use the **show ip interface** command in the EXEC mode.

show ip interface {**loopback-interface** *loopback-interface-number* | **vlan-interface** *vlan-interface-number* | **meth-interface***meth-interface-number*}

Syntax Description

loopback-interface-number	Displays information for the loopback interface.
vlan-interface-number	Displays information for the VLAN interface.
meth-interface-number	Displays information for the meth interface.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The followng example shows a sample output of a loopback interface:

```
Device# show ip interface loopback-interface 1
Show informations of interface
The mac-address of interface is 00:0a:5a:9b:18:15
Interface name      : LOOPBACK-IF1
Primary ipaddress   : None
Secondary ipaddress : None
Interface status    : Up


Total entries: 1 interface.
```

The followng example shows a sample output of a VLAN interface:

```
Device# show ip interface vlan-interface 1
Show informations of interface
The mac-address of interface is 00:0a:5a:9b:18:15
Interface description : interface1
Interface name        : VLAN-IF1
Primary ipaddress     : None
Secondary ipaddress   : None
VLAN                  : 1
Address-range         : 192.0.2.254-192.0.2.255,
Interface status      : Up


Total entries: 1 interface.
```

show ip source guard

To display the status and port filter applied on each port, use the **show ip-source-guard** command in privileged or global configuration mode.

```
show ip-source-guard [bind | permit | vlan]
```

Syntax Description

bind	Displays the entries of the static IP source binding table.
permit	Displays the whether Internet Group Management Protocol (IGMP) packets are permitted or not.
vlan ip *ip-address*	Displays VLAN information.

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show ip-source-guard
Port     Status   FilterType
g0/1     disable  N/A
g0/2     disable  N/A
g0/3     disable  N/A
g0/4     disable  N/A
g0/5     disable  N/A
g0/6     disable  N/A
g0/7     disable  N/A
g0/8     disable  N/A
e1/1     enable   ip+mac+vlan
e1/2     disable  N/A
e1/3     disable  N/A
e1/4     disable  N/A
e2/1     disable  N/A
e2/2     disable  N/A

Total entries:14
```

The following example displays the status of port filtering on IGMP packets:

```
Device#show ip-source-guard permit igmp

 IP source guard permit igmp status:disable
```

Related Commands

Command	Description
ip-source-guard	Configures the IP source guard function on the ports of the device.

show mac-address-table age-time

To display the aging time of the MAC address table, use the **show mac-address-table age-time** command in the EXEC mode.

show mac-address-table age-time

Syntax Description

age-time	Displays the aging time of the MAC address table.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The following example shows how to display the aging time for a MAC address table:

```
Device# show mac-address-table age-time

mac address table agingtime is 300 seconds.
```

show mac-address-table

To display information about the MAC address table, use the **show mac-address-table** command in the EXEC mode.

show mac-address-table {**static** | **permanent** | **dynamic**} **blackholelearning interface ethernet***interface-number* **vlan** *vlan-id*

Syntax Description

static	Displays the static MAC address table.
permanent	Displays the permanent entries in the MAC address table.
dynamic	Displays the dynamic MAC address table.
blackhole	Displays the blachole MAC address table.
learning	Displays the MAC address learning status.

Command Default

None

Command Modes

User EXEC
Priveleged EXEC

Examples

The following example shows how to display the dynamic MAC address table:

```
Device# show mac-address-table dynamic
Show ARL table information
MAC Address        VLAN ID  port  status
00:0a:5a:a7:01:34  100      g0/1  dynamic
00:0b:ab:82:2d:82  100      e1/3  dynamic
00:0c:29:07:b6:9b  100      e1/3  dynamic
00:0c:29:15:9e:10  100      e1/3  dynamic
00:0c:29:3c:3b:08  100      e1/3  dynamic
00:0c:29:3c:3b:12  100      e1/3  dynamic
00:0c:29:71:b1:4f  100      e1/3  dynamic
00:0c:29:71:b1:59  100      e1/3  dynamic
00:0c:29:b8:0f:0b  100      e1/3  dynamic
00:0c:29:b8:0f:15  100      e1/3  dynamic
00:11:32:47:9a:30  100      e1/3  dynamic
00:19:bb:2f:5a:81  100      e1/3  dynamic
00:19:bb:30:70:97  100      e1/3  dynamic
00:19:bb:30:a0:6b  100      e1/3  dynamic
00:1f:26:35:7a:9f  100      e1/3  dynamic
00:21:5a:a9:53:14  100      e1/3  dynamic
00:23:5d:fd:94:00  100      e1/3  dynamic
00:30:18:cc:7b:02  100      e1/3  dynamic
00:50:56:92:0a:09  100      e1/3  dynamic
00:50:56:92:88:2f  100      e1/3  dynamic
00:50:56:95:41:5e  100      e1/3  dynamic
00:50:56:bd:2b:cf  100      e1/3  dynamic
00:61:56:60:93:84  100      e1/3  dynamic
00:d0:0a:0b:ea:1c  100      e1/3  dynamic
00:e0:4c:86:70:01  100      e1/3  dynamic
00:eb:d5:5e:02:a0  100      e1/3  dynamic
0c:f5:a4:ba:44:9f  100      e1/3  dynamic
2c:ab:eb:22:76:8d  100      e1/3  dynamic
```

```
40:a6:e8:e6:52:de  100      e1/3  dynamic
40:a6:e8:e6:b5:5c  100      e1/3  dynamic
44:8a:5b:98:e9:60  100      e1/3  dynamic
5c:71:0d:bb:35:8b  100      e1/3  dynamic
5c:71:0d:bb:3c:19  100      e1/3  dynamic
5c:71:0d:bb:60:fa  100      e1/3  dynamic
68:9c:e2:a0:7d:3e  100      e1/3  dynamic
68:9c:e2:a0:7d:5e  100      e1/3  dynamic
68:ca:e4:3a:3d:e0  100      e1/3  dynamic
68:ef:bd:f0:d1:08  100      e1/3  dynamic
b0:7d:47:3f:47:ae  100      e1/3  dynamic
c8:f9:f9:45:12:5b  100      e1/3  dynamic
e4:1f:13:43:41:0a  100      e1/3  dynamic
e4:1f:13:77:9f:06  100      e1/3  dynamic
e4:1f:13:77:a0:c8  100      e1/3  dynamic
Total entries: 43 .
```

Examples

The following example shows how to display the static MAC address table:

```
Device# show mac-address-table static
Show ARL table information
MAC Address        VLAN ID  port  status
00:0a:5a:9b:18:15  1        cpu   static
00:0a:5a:9b:18:15  100      cpu   static
Total entries: 2 .
```

Examples

The following example shows how to display the MAC address table learning status:

```
Device# show mac-address-table learning interface ethernet 1/1
Port      Mac learning status
e1/1      enable
Total entries: 1 .
```

show mirror

To see the port mirror configuration, use the **show mirror** command in privileged or global configuration mode.

```
show mirror
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

```
Device#show mirror
Information about mirror port(s)
The monitor port            : e1/4
The mirrored egress ports   : cpu,e1/1-e1/2.
The mirrored ingress ports  : cpu,e1/1-e1/2.
```

show snmp community

To display the SNMP community strings configured on the switch, use the **show snmp community** command in privileged or global configuration mode.

```
show snmp community
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp community
Show snmp community information
Encryption status: OFF
index  community  priority  state   view-name
1      public     ro        permit  iso
2      private    rw        permit  iso
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string

show snmp contact

To display the SNMP contact string, use the **show snmp contact** command in privileged or global configuration mode.

```
show snmp contact
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp contact
Manager contact information : http://
```

Related Commands

Command	Description
snmp-server contact	Sets the SNMP manager contact information

show snmp engineid

To display the identification of the local SNMP engine and all remote engines that have been configured on the device, use the **show snmp engineid** command in privileged or global configuration mode.

```
show snmp engineid {local |remote }[engineid]
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

The following is a sample output of the **show snmp engineid local** command

```
Device#show snmp engineid local
Local engine id: : 134640000000000000000000
```

Related Commands

Command	Description
snmp-server engineid	Configures engine ID on the device.

show snmp group

To display the different SNMP group configurations, use the **show snmp group** command in privileged or global configuration mode.

```
show snmp group
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

Use this command to view the names of configured SNMP groups, the security models being used, and the different views configured under each group.

Example

```
Device#show snmp group
groupname: g3
securitymodel: 3 auth
readview: iso
writeview: iso
notifyview: no specified notifyview
context: default value(NULL)

groupname: initial
securitymodel: 3 noauthpriv
readview: iso
writeview: iso
notifyview: iso
context: default value(NULL)

groupname: initial
securitymodel: 3 auth
readview: iso
writeview: iso
notifyview: iso
context: default value(NULL)


group snmp3 number:3
```

Related Commands

Command	Description
snmp-server group	Configures an SNMP group

show snmp host

To display the recipient details for the SNMP trap notifications, use the **show snmp host** command in privileged or global configuration mode.

```
show snmp host
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp host
Show SNMP trap host information
SNMP host ip  security  version
10.75.166.19  public    2c
```

Related Commands

Command	Description
snmp-server host	Configures the recipient for the SNMP notifications.

show snmp location

To display the SNMP manager location string, use the **show snmp location** command in privileged or global configuration mode.

```
show snmp location
```

Command Default None

Command Modes Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp location
Switch location information : sample sysLocation factory default
```

Related Commands

Command	Description
snmp-server location	Sets the SNMP manager location string.

show snmp mib

To display the Management Information Base (MIB) module instance identifiers, use the **show snmp mib** command in privileged or global configuration mode.

```
show snmp mib [module module-name]
```

Syntax Description

module *module-name*	Specifies the MIB module object instance identifier

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Usage Guidelines

SNMP MIB is a repository for information about device parameters and network data. Collections of related objects are defined in MIB modules.

The **show snmp mib** command displays the instance identifiers for all the MIB objects on the system. The MIB module table names are registered when the system initializes.

Note The **show snmp mib** command generates a high volume of output if SNMP is enabled on your system.

Example

The following is a sample output that shows the details of the **gbnL2PppoePlus** MIB module:

```
Device#show snmp mib module gbnL2PppoePlus

gbnL2PppoePlus:pppoeplusType-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.2.0]
gbnL2PppoePlus:pppoeplusFormat-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.3.0]
gbnL2PppoePlus:pppoeplusDelimiter-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.4.0]
gbnL2PppoePlus:pppoeplusCircuitidOrder-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.5.0]
gbnL2PppoePlus:pppoeplusCircuitidString-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.6.0]
gbnL2PppoePlus:pppoeplusRemoteidOrder-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.7.0]
gbnL2PppoePlus:pppoeplusRemoteidString-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.8.0]
gbnL2PppoePlus:pppoeplusPortsIndex-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.1.1]
gbnL2PppoePlus:pppoeplusPortsOnOff-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.2.1]
gbnL2PppoePlus:pppoeplusPortsTrust-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.3.1]
gbnL2PppoePlus:pppoeplusPortsDropPadi-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.4.1]
gbnL2PppoePlus:pppoeplusPortsDropPado-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.5.1]
gbnL2PppoePlus:pppoeplusPortsStrategy-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.6.1]
gbnL2PppoePlus:pppoeplusPortsCircuit-[1.3.6.1.4.1.9.6.1.120.1.2.4.6.9.1.7.1]
```

show snmp name

To display the SNMP system name, use the **show snmp name** command in privileged or global configuration mode.

```
show snmp name
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp name
system name : 2
```

Related Commands

Command	Description
snmp-server name	Sets the SNMP system name.

show snmp notify

To display the configured SNMP notifications on the system, use the **show snmp notify** command in privileged or global configuration mode.

```
show snmp notify
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp notify
Name         Type  State
bridge       trap  enabled
gbn          trap  enabled
gbnsavecfg   trap  enabled
interfaces   trap  enabled
rmon         trap  enabled
snmp         trap  enabled
if-ethernet     Link-Trap
g0/1            enabled
g0/2            enabled
g0/3            enabled
g0/4            enabled
g0/5            enabled
g0/6            enabled
g0/7            enabled
g0/8            enabled
e1/1            enabled
e1/2            enabled
e1/3            enabled
e1/4            enabled
e2/1            enabled
e2/2            enabled
```

Related Commands

Command	Description
snmp-server trap-source	Configures an the interface that originates SNMP traps.
snmp-server enable	Enables SNMP notifications

show snmp user

To display information about the configured SNMP users, use the **show snmp user** command in privileged or global configuration mode.

```
show snmp user
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp user
User name: u3
Engine ID: 134640000000000000000000
Authentication Protocol: HMACMD5AuthProtocol
Group-name: g3
Validation: valid

User name: initialmd5
Engine ID: 134640000000000000000000
Authentication Protocol: HMACMD5AuthProtocol
Group-name: initial
Validation: valid

User name: initialsha
Engine ID: 134640000000000000000000
Authentication Protocol: HMACSHAAuthProtocol
Group-name: initial
Validation: valid

User name: initialnone
Engine ID: 134640000000000000000000
Authentication Protocol: NoauthProtocol
Group-name: initial
Validation: valid

user number:4
```

Related Commands

Command	Description
snmp-server user	Configures an SNMP user in a group.

show snmp view

To display the details of an SNMP view, use the **show snmp view** command in privileged or global configuration mode.

```
show snmp view[view-name]
```

Command Default

None

Command Modes

Privileged (#)

Global Configuration (config)

Example

```
Device#show snmp view
View Name  Type     Subtree
iso        Include  1
sysview    Include  1.3.6.1.2.1.1
internet   Include  1.3.6.1

view number:3
```

Related Commands

Command	Description
snmp-server view	Configures an SNMP view

shutdown

To shut down a VLAN interface, use the **shutdown** command in the VLAN configuration mode. You can cancel the shuydown of the VLAN interface by using the **no** form of the command.

shutdown

no shutdown

Syntax Description

shutdown	Shuts down the VLAN interface.

Command Default

None

Command Modes

VLAN configuration

Examples

The following example shows how to shut down a VLAN interface:

```
Device(config-if-vlanif)# shutdown
```

snmp-server

To enable or disable Simple Network Management Protocol (SNMP) on a device use the **snmp-server** command in the global configuration mode.

```
snmp-server {enable [informs |traps][bridge | gbn | gbnsavecfg | interfaces
| rmon | snmp]] | disable}
```

Syntax Description

enable	Enables SNMP traps on the device
disable	Disables the SNMP server
informs	Configures SNMP inform request
traps	Configures SNMP trap notifications

- **bridge** Specifies the type of SNMP informs or traps notifications to be enabled.
- **gbn** If you do not specify the type of SNMP inform or trap, all traps and informs that are configured on your system are enabled.
- **gbnsavecfg**
- **interfaces**
- **rmon**
- **snmp**

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The **snmp-server enable** command is optional. SNMP traps and informs are enabled by default, on the device. Use the **snmp-server disable** command to disable SNMP traps or informs on the device.

Example

```
Device#configure terminal
Device(config)#snmp-server enable traps gbn
```

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP) use the **snmp-server community** command in the global configuration mode. To remove the configured community string, use the **no** form of the command.

```
[no] snmp-server community  {name|md5 }{ro|rw}{deny|permit}[view view-name]
```

Syntax Description

name	SNMP community name that consists of 1 to 32 characters
md5	Uses md5 for authentication
ro	Specifies read-only access. Authorized management stations can retrieve only MIB objects
rw	Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
permit	Specifies community name string is active
deny	Specifies community name string is not activated
view *view-name*	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community. Default view is ISO.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The SNMP community name authenticates access to MIB objects. In order for the NMS to access the switch, the community name definitions on the NMS must match at least one of the community name definitions on the switch.

Examples

The following example shows how to set the read/write community string to group1:

```
Device#configure terminal
Device(config)#snmp-server community group1 rw permit
```

The following example shows how to assign the string manager to SNMP and allow read-only access to the objects in the view called restricted:

```
Device(config)#snmp-server community group1 ro permit view restricted
```

The following example shows how to remove the community 1:

```
Device(config)#no snmp-server community 1
```

snmp-server community encrypt

To enable or disable encryption of community access string, use the **snmp-server community encrypt** command in the global configuration mode.

```
snmp-server community encrypt  {enable|disable }
```

Syntax Description

enable	Enables encryption of the community name string
disable	Disables encryption of community name string

Command Default

The community name string is not encrypted.

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#snmp-server community encrypt enable
```

snmp-server contact

To configure the SNMP manager contact information, use the **snmp-server contact** command in the global configuration mode. To remove the SNMP manager contact information, use the **no** form of the command.

`snmp-server contact` *contact-information*

Syntax Description

contact-information	Specifies the SNMP manager contact details

Command Default

SNMP manager contact string is not set.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server contact SystemOperator
```

snmp-server encrypt

To enable or disable the encryption of the password for a user, use the **snmp-server encrypt** command in the global configuration mode.

A password is encrypted by default.

```
snmp-server encrypt {enable|disable}
```

Syntax Description

enable	Enables the encryption of password
disable	Disables the encryption of password

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#snmp-server encrypt disable
```

snmp-server engineid

To configure the Simple Network Management Protocol (SNMP) engine ID on a local device or a remote device, use the **snmp-server** command in the global configuration mode.

`snmp-server engineid local` *engineid* `|` `remote` *ip-address* `[udp-port`*port-num*`]` *engineid*

Syntax Description

local *engineid*	Specifies the engine ID of the local device
remote *ip-address*	Specifies the engine ID of the local device
udp-port*port-num*	Specifies the UDP port on the remote device

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

An SNMP engine ID is a unique string that identifies the device, for administrative purposes.

The engine ID of the local SNMP device is 134640000000000000000000. You can modify the local engine ID, but not delete it. You can create and delete the engine ID of a remote SNMP device. If you delete a remote engine ID, the corresponding users are also deleted. You can configure a maximum number of 32 remote engine IDs.

Example

```
Device#configure terminal
Device(config)#snmp-server engineid remote 172.16.20.4 1
```

snmp-server group

To configure an SNMP group that enables authentication for the members of a specified view, use the **snmp-server group** command in the global configuration mode. To remove the configured authentication for the SNMP group, use the **no** form of the command.

`[no] snmp-server group` *group-name*`3 [auth |noauthpriv |priv] read` *read-view* `write` *write-view* `notify` *notify-view*

Syntax Description

auth	Specifies that packets are authenticated but not encrypted.
noauthpriv	Specifies that packets are not authenticated.
priv	Specifies that packets are authenticated and not encrypted.
read *read-view*	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent. If a *read-view* is not specified, it defaults to the iso view and auth security level.
write *write-view*	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent. **write-view** does not have defaults. Hence it is mandatory to specify it if **write** is configured.
notify *notify-view*	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notification or a trap. **notify-view** does not have defaults. Hence it is mandatory to specify *notify-view* if **notify** is configured.

Command Default

None

Command Modes

Global configuration (config)

Examples

```
Device#configure terminal
Device(config)#snmp-server group g1 3 priv write dept-view
```

snmp-server host

To configure the recipient of an SNMP notification operation, use the **snmp-server host** command in the global configuration mode. To remove the configured recipient for the SNMP group, use the **no** form of the command.

```
[no] snmp-server host {inet6 ipv6-address |ipv4-address}{version {1 | 2c | 3{auth
| noauthpriv | priv }} }security-name [udp-port udp-port-num][ notify-type[bridge
| gbn | gbnsavecfg | interfaces | rmon | snmp] ]
```

Syntax Description

inet6 *ipv6-address*	Specifies the IPv6 address of the recipient of SNMP traps
ipv4-address	Specifies the IPv4 address of the recipient of SNMP traps
version {**1** | **2c** | **3**{**auth** | **noauthpriv** | **priv** }	Specifies the SNMP version: 1, 2c, 3. If you specify SNMP version 3, ensure that you specify the security levels too: • **auth**: Enables MD5 and SHA packet authentication • **noauth**: Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. • **priv**: Enables Data Encryption Standard (DES) packet encryption.
security-name	Defines a name for this configuration.
udp-port *udp-port-num*	Specifies the UDP port on the host device.
notify-type	Specifies the type of notification to be sent to the host: • bridge • gbn • gbnsavecfg • interfaces • rmon • snmp

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use the **snmp-server host** command to configure a recipient for the SNMP notifications. If this command is not configured, no notifications are sent. **snmp-server host** command is used in conjunction with the **snmp-server enable** command. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Examples

```
Device#configure terminal
Device(config)#snmp-server host 192.168.5.1 version 2c test-sec udp-port 4
```

snmp-server location

To set the SNMP server location string, use the **snmp-server location** command in the global configuration mode. To remove the SNMP server location information, use the **no** form of the command.

```
[no] snmp-server location syslocation
```

Syntax Description

syslocation	String that describes the SNMP server location

Command Default

No system location string is set.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server location Building13
```

snmp-server max-packet-length

To configure the maximum size of SNMP packets, use the **snmp-server max-packet-length** command in the global configuration mode. To remove the maximum packet length configuration for SNMP packets, use the **no** form of the command.

```
[no] snmp-server max-packet-length length
```

Syntax Description

length	Specifies the maximum packet length for SNMP packets. The value ranges from 484 bytes through 8000 bytes. Default value is 1000 bytes.

Command Default

Maximum packet length is set to 1000 bytes.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server max-packet-length 1200
```

snmp-server name

To set the SNMP system name string, use the **snmp-server name** command in the global configuration mode. To remove the SNMP server name information, use the **no** form of the command.

```
[no] snmp-server name sysname
```

Syntax Description

sysname	String that describes the SNMP server name

Command Default

No system name string is set.

Command Modes

Global Configuration (config)

Example

```
Device(config)#snmp-server name Building13Server
```

snmp-server trap-source

To specify the interface from which the Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in the global configuration mode. To remove the source of SNMP trap, use the **no** form of the command.

`snmp-server trap-source {inet6 |vlan-interface` *vlan-id*`|loopback-interface` *interface*`|vlan-interface` *vlan-id*`}`

Syntax Description

inet6	Specifies the IPv6 address family
vlan-interface *vlan-id*	Specifies the VLAN id to which the VLAN interfaces that originate the traps, belong.
loopback-interface *interface*	Specifies the loopback interface that is configured as the origin of the traps.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to monitor notifications from a particular interface.

An SNMP trap or inform that is sent from an SNMP server has a notification address of the interface it went out of at that time.

Example

```
Device#configure terminal
Device(config)#snmp-server trap-source vlan-interface 3
```

snmp-server user

To configure a new user to an SNMP group, use the **snmp-server user** command in the global configuration mode. To remove a configured user from an SNMP group, use the **no** form of this command.

`[no]snmp-server user` *username group-name* `[remote` *ipaddress* `[udp-port` *port-number* `] ] [auth {md5 |sha }{auth-password {authpassword |encrypt-authpassword` *password*`} |auth-key{`*authkey* `| encrypt-authkey`*password*`}}[privdes {priv-key{`*key*`| encrypt-privkey`*key*`}| priv-password{`*password* `| encrypt-privpassword`*privpassword*`} } ] ]`

Syntax Description

username	Name of the user created
group-name	Name of the SNMP group to which the user belongs
remote	(Optional) A remote SNMP entity to which the user belongs
ipaddress	(Optional) IP address of the remote SNMP host.
udp-port *port-number*	(Optional) UDP port on the remote port
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level
sha	(Optional) Specifies the HMAC-SHA-96 authentication level
auth-password *authpassword*	Specifies the authentication password
auth-key *authkey*	Specifies the authentication key
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
priv-key	(Optional) String that specifies the privacy user password.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The **snmp-server user** command configures a user for a local engine or a remote engine.

The following three users exist by default and they are reserved as the system users:

- initialmd5
- initialsha
- initialnone

To configure a remote engine user, specify remote ipaddress. If you do not specify remote ipaddress, a local engine user is configured.

For a remote user, the default port number is 162. To configure a different remote port, specify a udp-port port-number .

Three levels of user privileges can be specified:

- **noauthpriv** : Authentication and password encryption are not required. It is the default configuration.
- **auth**: Authentication is required but password encryption is not required.
- **authpriv**: Authentication and password encryption, both are required.

Note The user security level should be the same as the corresponding group security level.

Example

```
Device#configure terminal
Device(config)#snmp-server user u3 g3 auth md5 auth-password password1
```

snmp-server view

To create or update an SNMP server view, use the **snmp-server view** command in the global configuration mode. To remove the configured SNMP server view, use the **no** form of the command.

```
[no] snmp-server view view-name oid-subtree {include | exclude}
```

Syntax Description

oid-subtree	Object identifier (OID) of the ASN.1 subtree that is either included or excluded from the view. A string that can have upto to 64 characters.
view-name	Name of the SNMP view that is to be created.
exclude	Excludes the OID specified in the *oid-subtree* argument from the SNMP view.
include	Includes the OID specified in the *oid-subtree* argument in the SNMP view.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

Use this command to create a view that is a list of SNMP object trees, which you can access. The **iso**, **internet** and **sysview** views exist by default. You cannot delete or modify the **internet** view.

Examples

The following example creates a view named **oneview** and excludes all objects of the subtree:

```
Device#configure terminal
Device(config)#snmp-server view oneview 1.3 exclude
```