I Commands

This chapter describes the Cisco Nexus 1000V commands that begin with the letter I.

inherit port-profile

To add the inherited configuration to the new port profile as a default configuration, use the **inherit port-profile** command. To remove the inherited policies, use the **no** form of this command.

inherit port-profile *name*

no inherit port-profile

Syntax Description

name	Port profile name whose policies are inherited. The name has a maximum length of 80, case-sensitive, alphanumeric characters and must be unique for each port profile on the Cisco Nexus 1000V.

Defaults

None

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Usage Guidelines

Any inherited setting, except the port profile type, can be changed using the command-line interface (CLI).

When you use the no form of this command, the port profile settings are returned to the defaults, except for the port profile type and any settings that were explicitly configured independent of those inherited.

Examples

This example shows how to designate *AllAccess1* as the port profile whose policies will be inherited:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-profile type vethernet AllAccess2
n1000v(config-port-prof)# inherit port-profile AllAccess1
```

This example shows how to remove the inherited policies:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-profile type vethernet AllAccess2
n1000v(config-port-prof)# no port-profile inherit
```

Related Commands

Command	Description
port-profile	Places you into port profile configuration mode and defines the port profile.
show port-profile	Displays the port profile inherited by the current port profile.

install license bootflash:

To install a license file(s) on a Virtual Supervisor Module (VSM), use the **install license bootflash:** command.

install license bootflash: *filename*

Syntax Description

filename	(Optional) License file name. If you do not specify a name, then the license is installed using the default name. The filename is alphanumeric, case-sensitive and can be up to 28 characters.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Usage Guidelines

Follow these guidelines:

- You must first uninstall an evaluation license if one is present on your Virtual Supervisor Module (VSM). For more information, see the *Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(5.1)*.
- You must be logged in to the active VSM console port.
- This command installs the license file using the name, license_file.lic. You can specify a different name.
- If you are installing multiple licenses for the same VSM, also called license stacking, make sure that each license key filename is unique.
- Repeat this procedure for each additional license file you are installing, or stacking, on the VSM.

Examples

This example shows how to install a license to bootflash on a VSM and then display the installed file:

```
n1000v# install license bootflash:license_file.lic
Installing license ..done
n1000v# show license file license.lic
SERVER this_host ANY
VENDOR cisco
INCREMENT NEXUS1000V_LAN_SERVICES_PKG cisco 1.0 permanent 1 \
    HOSTID=VDH=1575337335122974806 \
    NOTICE="<LicFileID>license.lic</LicFileID><LicLineID>0</LicLineID> \
    <PAK>PAK12345678</PAK>" SIGN=3AF5C2D26E1A
n1000v#
```

Related Commands

Command	Description
clear license	Uninstalls a license, that is, removes it from the VSM and shuts down the Ethernet interfaces to the VEM covered by that license.
install license	Installs a license file(s) on a VSM
logging level license	Designates the level of severity at which license messages should be logged.
show license file	Verifies the license installation by displaying the license configured for the VSM.
svs license transfer src-vem	Transfers licenses from a source VEM to another VEM or to the VSM pool of available licenses.

interface control0

To configure the control interface and enter interface configuration mode, use the **interface control0** command.

interface control0

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)
Interface configuration (config-if)

SupportedUserRoles

network-admin

Examples

This example shows how to enter interface configuration mode to configure the control interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface control0
n1000v(config-if)#
```

Related Commands

Command	Description
show interface control0	Displays information about the traffic on the control interface.

interface ethernet

To configure an Ethernet interface, use the **interface ethernet** command.

interface ethernet *slot/port*

Syntax Description		
	slot/port	Slot number and port number for the Ethernet interface. The slot number ranges from 1 to 66 and the port number from 1 to 128. The slot and port numbers must be separated by the slash (/) operator.

Defaults

None

Command Modes

Global configuration (config)

Interface configuration (config-if)

SupportedUserRoles

network-admin

Examples

This example shows how to access interface command mode for configuring the Ethernet interface on slot 2, port 1:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface ethernet 2/1
n1000v(config-if)#
```

Related Commands

Command	Description
show interface ethernet	Displays information about the Ethernet interface.

interface mgmt0

To configure the management interface and enter interface configuration mode, use the **interface mgmt0** command.

interface mgmt0

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)
Interface configuration (config-if)

SupportedUserRoles

network-admin

Examples

This example shows how to enter interface configuration mode to configure the management interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface mgmt0
n1000v(config-if)#
```

Related Commands

Command	Description
show interface mgmt0	Displays information about the traffic on the management interface.

interface port-channel

To create a port channel interface and enter interface configuration mode, use the **interface port-channel** command. To remove a logical port channel interface or subinterface, use the **no** form of this command.

interface port-channel *channel-number*

no interface port-channel *channel-number*

Syntax Description

channel-number	Channel number that is assigned to this port channel logical interface. The range is from 1 to 4096.

Defaults

None

Command Modes

Global configuration (config)
Interface configuration (config-if)

SupportedUserRoles

network-admin

Usage Guidelines

Use the **interface port-channel** command to create or delete port channel groups and to enter interface configuration mode for the port channel.

A port can belong to only one channel group.

When you use the **interface port-channel** command, follow these guidelines:

- If you are using the Cisco Discovery Protocol (CDP), you must configure it only on the physical interface and not on the port channel interface.
- If you do not assign a static MAC address on the port channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the port channel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

Examples

This example shows how to create a port channel group interface with channel group number 50:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface port-channel 50
n1000v(config-if)#
```

Related Commands

Command	Description
show interface port-channel	Displays information on traffic on the specified port channel interface.
show port-channel summary	Displays information about the port channels.

interface vethernet

To create a virtual Ethernet interface and enter interface configuration mode, use the **interface vethernet** command. To remove a virtual Ethernet interface, use the **no** form of this command.

interface vethernet *number*

no interface vethernet *number*

Syntax Description

number	Interface number. The range is from 1 to 1048575.

Defaults

None

Command Modes

Global configuration (config)
Interface configuration (config-if)

SupportedUserRoles

network-admin

Usage Guidelines

Use the **interface vethernet** command to create a virtual Ethernet interface.

Examples

This example shows how to create a virtual Ethernet interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface vethernet 50
n1000v(config-if)#
```

Related Commands

Command	Description
show interface vethernet	Displays information about the traffic on the specified virtual Ethernet interface.

ip access-group

To create an IP access group for the mgmt0 interface, use the **ip access-group** command. To remove the access group, use the **no** form of this command.

ip access-group *name* {**in** | **out**}

no ip access-group *name* {**in** | **out**}

Syntax Description

name	List name. The list name is alphanumeric, case-sensitive and can be up to 28 characters.
in	Specifies the incoming (ingress) traffic direction.
out	Specifies the outgoing (egress) traffic direction.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Examples

This example shows how to configure an IP access group named Telnet for incoming traffic to the mgmt0 interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface mgmt0
n1000v(config-if)# ip access-group telnet in
n1000v(config-if)#
```

Related Commands

Command	Description
show ip access-lists	Displays the ACL configuration.

ip access-list

To create an access list, use the **ip access-list** command. To remove an access list, use the **no** form of this command.

ip access-list {*name* | **match-local-traffic**}

no ip access-list {*name* | **match-local-traffic**}

Syntax Description

name	List name. The list name is alphanumeric, case-sensitive and can be up to 28 characters.
match-local-traffic	Enables access list matching for locally generated traffic.

Defaults

No access list exists.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Examples

This example shows how to create an access list:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip access-list acl1
n1000v(config)#
```

Related Commands

Command	Description
show access-lists	Displays access lists.

ip route

To create an IP route, use the **ip route** command. To remove an IP route, use the **no** form of this command.

ip route {*address mask* | *prefix*} {*next-hop* | *next-hop-prefix* | *interface-type interface-number*} [**tag** *tag-value* | *preference*]

no ip route {*address mask* | *prefix*} {*next-hop* | *next-hop-prefix* | *interface-type interface-number*} [**secondary** | **tag** *tag-value* | *preference*]

Syntax Description

address	IP address in the format A.B.C.D.
mask	IP network mask in the format A.B.C.D.
prefix	IP prefix and network mask length in the format A.B.C.D/LEN.
next-hop	IP next-hop address in the format A.B.C.D.
next-hop-prefix	IP next-hop prefix in the format A.B.C.D./LEN.
interface-type	Specifies an interface type.
interface-number	Interface or subinterface number.
secondary	(Optional) Configures additional IP addresses on the interface.
tag	(Optional) Specifies a supply tag.
tag-value	Supply tag value. The range is from 0 to 4294967295. The default is 0.
preference	(Optional) Route preference.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Examples

This example shows how to create an IP address:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip route 10.1.1.0 255.255.255.0 10.1.1.10
n1000v(config)#
```

Related Commands

Command	Description
show ip interface A.B.C.D.	Displays interfaces for local IP addresses.

ip arp inspection limit

To set the rate limit of the Address Resolution Protocol (ARP) requests and responses, use the **ip arp inspection limit** command. To remove this setting, use the **no** form of this command. To set the rate limit to its default, use the **default** form of this command.

ip arp inspection limit {**rate** *pps* [**burst interval** *bint*] | **none**}

no ip arp inspection limit {**rate** *pps* [**burst interval** *bint*] | **none**}

default ip arp inspection limit {**rate** *pps* [**burst interval** *bint*] | **none**}

Syntax Description

rate *pps*	Specifies the rate limit in packets per second.
burst interval	(Optional) Specifies the burst interval.
bint	(Optional) Burst interval in seconds.
none	Specifies that there is no limit.

Defaults

None

Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Examples

This example shows how to set the rate limit of ARP requests to 20 pps:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip arp inspection limit rate 20
```

This example shows how to remove the configuration:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no arp inspection limit rate 20
```

Related Commands

Command	Description
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.

ip arp inspection trust

To configure a Layer 2 interface as a trusted Address Resolution Protocol (ARP) interface, use the **ip arp inspection trust** command. To configure a Layer 2 interface as an untrusted ARP interface, use the **no** form of this command. To return a Layer 2 interface to its default, use the **default** form of this command.

ip arp inspection trust

no ip arp inspection trust

default ip arp inspection trust

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all interfaces are untrusted ARP interfaces.

Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Usage Guidelines

You can configure only Layer 2 virtual Ethernet interfaces as trusted ARP interfaces.

Examples

This example shows how to configure a Layer 2 interface as a trusted ARP interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip arp inspection trust
n1000v(config-if)#
```

Related Commands

Command	Description
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.

ip arp inspection validate

To enable additional Dynamic Address Resolution Protocol (ARP) Inspection (DAI) validation, use the **ip arp inspection validate** command. To disable additional DAIs, use the **no** form of this command.

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**] | **ip** [**dst-mac**] [**src-mac**] | **src-mac** [**dst-mac**] [**ip**]}

no ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**] | **ip** [**dst-mac**] [**src-mac**] | **src-mac** [**dst-mac**] [**ip**]}

Syntax Description

dst-mac	(Optional) Enables validation of the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. The device classifies packets with different MAC addresses as invalid and drops them.
ip	(Optional) Enables validation of the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The device checks the sender IP addresses in all ARP requests and responses and checks the target IP addresses only in ARP responses.
src-mac	(Optional) Enables validation of the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. The devices classifies packets with different MAC addresses as invalid and drops them.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Usage Guidelines

You must specify at least one keyword. If you specify more than one keyword, the order is irrelevant.

Examples

This example shows how to enable additional DAI validation:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip arp inspection validate src-mac dst-mac ip
n1000v(config)#
```

Related Commands

Command	Description
show ip arp inspection statistics	Displays the DAI configuration status.

ip arp inspection vlan

To enable dynamic Address Resolution Protocol (ARP) inspection (DAI) for a list of VLANs, use the **ip arp inspection vlan** command. To disable DAI for a list of VLANs, use the **no** form of this command.

ip arp inspection vlan *vlan-list*

no ip arp inspection vlan *vlan-list*

Syntax Description

vlan-list	VLANs on which DAI is active. The *vlan-list* argument allows you to specify a single VLAN identification number, a range of VLAN identification numbers, or comma-separated IDs and ranges (see the "Examples" section). The range is from 1 to 4096.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Usage Guidelines

By default, the device does not log packets inspected by DAI.

Examples

This example shows how to enable DAI on VLANs 13, 15, and 17 through 23:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip arp inspection vlan 13,15,17-23
n1000v(config)#
```

Related Commands

Command	Description
ip arp inspection validate	Enables additional DAI validation.
show ip arp inspection vlan	Displays the DAI status for a specified list of VLANs.

ip dhcp snooping

To globally enable Dynamic Host Configuration Protocol (DHCP) snooping, use the **ip dhcp snooping** command. To globally disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping

no ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

By default, DHCP snooping is globally disabled.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Usage Guidelines

To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).

The device preserves the DHCP snooping configuration when you disable DHCP snooping with the **no ip dhcp snooping** command.

Examples

This example shows how to globally enable DHCP snooping:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip dhcp snooping
n1000v(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.

ip dhcp snooping information option

To relay the Virtual Supervisor Module (VSM) MAC address and virtual Ethernet port information in Dynamic Host Configuration Protocol (DHCP) packets, use the **ip dhcp snooping information option** command. To remove the configuration, use the **no** form of this command.

ip dhcp snooping information option

no ip dhcp snooping information option

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Examples

This example shows how to globally relay the VSM MAC address and virtual Ethernet port information in DHCP packets:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip dhcp snooping information option
n1000v(config)#
```

This example shows how to remove global relaying of the VSM MAC address and virtual Ethernet port information in DHCP packets:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no ip dhcp snooping information option
n1000v(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.

ip dhcp snooping limit rate

To configure a rate limit for Dynamic Host Configuration Protocol (DHCP) packets that are received on a port, use the **ip dhcp snooping limit rate** command. To remove the rate limit for DHCP packets that are received on each port, use the **no** form of this command. To restore the default setting, use the **default** form of this command.

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate

default ip dhcp snooping limit rate

Syntax Description

rate	DHCP packets per second. The range is from 1 to 2048.

Defaults

None

Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Examples

This example shows how to limit the rate of DHCP packets to 30 packets per-second on virtual Ethernet interface 3:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface vethernet 3
n1000v(config-if)# ip dhcp snooping limit rate 30
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.

ip dhcp snooping trust

To configure an interface as a trusted source of Dynamic Host Configuration Protocol (DHCP) messages, use the **ip dhcp snooping trust** command. To configure an interface as an untrusted source of DHCP messages, use the **no** form of this command. To restore the default setting, use the **default** form of this command.

ip dhcp snooping trust

no ip dhcp snooping trust

default ip dhcp snooping trust

Syntax Description

This command has no arguments or keywords.

Defaults

By default, no interface is a trusted source of DHCP messages.

Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Usage Guidelines

You can configure DHCP trust on the following types of interfaces:

- Layer 2 virtual Ethernet interfaces
- Private VLAN interfaces

Examples

This example shows how to configure an interface as a trusted source of DHCP messages:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip dhcp snooping trust
n1000v(config-if)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping verify mac-address	Enables MAC address verification as part of DHCP snooping.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.

ip dhcp snooping verify mac-address

To enable Dynamic Host Configuration Protocol (DHCP) snooping for MAC address verification, use the **ip dhcp snooping verify mac-address** command. To disable MAC address verification, use the **no** form of this command.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Examples

This example shows how to enable DHCP snooping for MAC address verification:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip dhcp snooping verify mac-address
n1000v(config)#
```

This example shows how to disable DHCP snooping for MAC address verification:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no ip dhcp snooping verify mac-address
n1000v(config)#
```

Related Commands

Command	Description
clear ip dhcp snooping binding	Clears dynamically added entries from the DHCP snooping binding database.
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Enables DHCP snooping globally.
ip dhcp snooping limit rate	Configures the DHCP limit rate.
ip dhcp snooping trust	Configures the interface as a trusted interface for DHCP snooping.
ip dhcp snooping verify mac-address	Enables DHCP snooping MAC address verification.

Command	Description
ip dhcp snooping vlan	Enables DHCP snooping on the VLANs specified by *vlan-list*.
show running-config dhcp	Displays the DHCP snooping configuration.

ip dhcp snooping vlan

To enable Dynamic Host Configuration Protocol (DHCP) snooping on one or more VLANs, use the **ip dhcp snooping vlan** command. To disable DHCP snooping on one or more VLANs, use the **no** form of this command.

ip dhcp snooping vlan *vlan-list*

no ip dhcp snooping vlan *vlan-list*

Syntax Description

vlan-list	VLANs on which to enable DHCP snooping. The *vlan-list* argument allows you to specify a single VLAN identification number, a range of VLAN identification numbers, or comma-separated IDs and ranges (see the "Examples" section). The range is from 1 to 4096.

Defaults

By default, DHCP snooping is not enabled on any VLAN.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Examples

This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip dhcp snooping vlan 100,200,250-252
n1000v(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
show ip dhcp snooping	Displays general information about DHCP snooping.

ip directed-broadcast

To enable IP directed broadcast, use the **ip directed-broadcast** command. To disable IP directed broadcast, use the **no** form of this command.

ip directed-broadcast

no ip directed-broadcast

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Examples

This example shows how to enable IP directed broadcast:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface mgmt 0
n1000v(config-if)# ip directed-broadcast
n1000v(config-if)#
```

Related Commands

Command	Description
show ip interface	Displays IP interface information.

ip dscp

To specify the IP Differentiated Services Code Point (DSCP) value for the packets in the Encapsulated Remote Switch Port Analyzer (ERSPAN) traffic and save it in the running configuration, use the **ip dscp** command.

ip dscp *dscp_value*

Syntax Description

dscp_value	DSCP value, in seconds, for ERSPAN traffic packets. The range is from 0 to 63.

Defaults

The default DSCP value is 0.

Command Modes

Command-line interface (CLI) ERSPAN source configuration (config-erspan-src)

SupportedUserRoles

network-admin

Examples

This example shows how to specify the DSCP value of 25 for packets in the ERSPAN traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# monitor session 3 type erspan
n1000v(config-erspan-src)# ip dscp 25
n1000v(config-erspan-src)#
```

Related Commands

Command	Description
description	For the specified ERSPAN session, adds a description and saves it in the running configuration.
destination ip	Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration.
erspan-id	Adds an ERSPAN ID to the session configuration and saves it in the running configuration.
filter vlan	Configures the VLANs, VLAN lists, or VLAN ranges to be monitored for the specified session, and saves this information in the running configuration.
ip prec	Specifies the IP precedence value for the packets in the ERSPAN traffic, and saves it in the running configuration.
ip ttl	Specifies the IP time-to-live value for the packets in the ERSPAN traffic, and saves it in the running configuration.
monitor session type erspan-source	Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode.
no shut	Enables the ERSPAN session and saves it in the running configuration.

Command	Description
show monitor session session_id	Displays the ERSPAN session configuration as it exists in the running configuration.
source	Configures the sources and the direction of traffic to monitor for the specified session, and saves the information in the running configuration.

ip flow monitor

To enable a Flexible NetFlow flow monitor for traffic that the router is receiving or forwarding, use the **ip flow monitor** command. To disable a Flexible NetFlow flow monitor, use the **no** form of this command.

ip flow monitor *monitor-name* {**input** | **output**}

no ip flow monitor *monitor-name* {**input** | **output**}

Syntax Description

monitor-name	Flow monitor name. The name is alphanumeric, case-sensitive, and has a maximum of 63 characters.
input	Monitors traffic that the router is receiving on the interface.
output	Monitors traffic that the router is transmitting on the interface.

Defaults

Disabled.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Usage Guidelines

You must have already created a flow monitor by using the **flow monitor** command before you can apply the flow monitor to an interface with the **ip flow monitor** command to enable traffic monitoring with Flexible NetFlow.

Examples

This example shows how to enable a flow monitor for monitoring input traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

This example shows how to enable a flow monitor for monitoring output traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

This example shows how to enable the same flow monitor on the same interface for monitoring input and output traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

This example shows how to enable two different flow monitors on the same interface for monitoring input and output traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

This example shows how to enable the same flow monitor on two different interfaces for monitoring input and output traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config)# interface ethernet1/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

This example shows how to enable two different flow monitors on two different interfaces for monitoring input and output traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config)# interface ethernet1/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor	Creates a flow monitor.
flow record	Creates a flow record.

ip igmp snooping (Global)

To enable Internet Group Management Protocol (IGMP) snooping, use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Usage Guidelines

If the global configuration of IGMP snooping is disabled, all VLANs are treated as disabled, whether they are enabled or not.

Examples

This example shows how to enable IGMP snooping:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip igmp snooping
n1000v(config)#
```

This example shows how to disable IGMP snooping:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no ip igmp snooping
n1000v(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping (VLAN)

To enable Internet Group Management Protocol (IGMP) snooping on a VLAN interface, use the **ip igmp snooping** command. To disable IGMP snooping on the interface, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Usage Guidelines

If the global configuration of IGMP snooping is disabled, all VLANs are treated as disabled, whether they are enabled or not.

Examples

This example shows how to enable IGMP snooping on a VLAN interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping
n1000v(config-vlan)#
```

This example shows how to disable IGMP snooping on a VLAN interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# no ip igmp snooping
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping explicit-tracking

To enable tracking of Internet Group Management Protocol Version 3 (IGMPv3) membership reports from individual hosts for each port on a per-VLAN basis, use the **ip igmp snooping explicit-tracking** command. To disable tracking, use the **no** form of this command.

ip igmp snooping explicit-tracking

no ip igmp snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

VLAN feature configuration (config-vlan-config)

SupportedUserRoles

network-admin

Examples

This example shows how to enable tracking of IGMPv3 membership reports on a VLAN interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 1
n1000v(config-vlan-config)# ip igmp snooping explicit-tracking
n1000v(config-vlan-config)#
```

This example shows how to disable IGMP snooping on a VLAN interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 1
n1000v(config-vlan-config)# no ip igmp snooping explicit-tracking
n1000v(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping fast-leave

To enable support of Internet Group Management Protocol Version 2 (IGMPv2) hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol, use the **ip igmp snooping fast-leave** command. To disable support of IGMPv2 hosts, use the **no** form of this command.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Usage Guidelines

When you enable fast leave, the IGMP software assumes that only one host is present on each VLAN port.

Examples

This example shows how to enable support of IGMPv2 hosts:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping fast-leave
n1000v(config-vlan)#
```

This example shows how to disable support of IGMPv2 hosts:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# no ip igmp snooping fast-leave
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping last-member-query-interval

To configure a query interval in which the software removes a group, use the **ip igmp snooping last-member-query-interval** command. To reset the query interval to the default, use the **no** form of this command.

ip igmp snooping last-member-query-interval *interval*

no ip igmp snooping last-member-query-interval [*interval*]

Syntax Description

interval	Query interval in seconds. The range is from 1 to 25. The default is 1.

Defaults

The query interval is 1.

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Examples

This example shows how to configure a query interval in which the software removes a group:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping last-member-query-interval 3
n1000v(config-vlan)#
```

This example shows how to reset a query interval to the default:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# no ip igmp snooping last-member-query-interval
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping link-local-groups-suppression (VLAN)

To suppress snooping on link-local group IP addresses use the **ip igmp snooping link-local-groups-suppression** command. To allow unlimited snooping, use the **no** form of this command.

ip igmp snooping link-local-groups-suppression

no ip igmp snooping link-local-groups-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Usage Guidelines

You can apply link-local groups suppression to all interfaces in the Virtual Supervisor Module (VSM) by entering this command in global configuration mode.

Examples

This example shows how to limit Internet Group Management Protocol (IGMP) traffic sent from VLAN 342:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping link-local-groups-suppression
```

This example shows how to resume IGMP traffic sent from VLAN 342:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan vlan2
n1000v(config-vlan)# no ip igmp snooping link-local-groups-suppression
n1000v(config-vlan)#
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on a VLAN.
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping link-local-groups-suppression (Global)

To suppress snooping on link-local group IP addresses, use the **ip igmp snooping link-local-groups-suppression** command. To allow unlimited snooping, use the **no** form of this command.

ip igmp snooping link-local-groups-suppression

no ip igmp snooping link-local-groups-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Usage Guidelines

You can apply link-local groups suppression to a single VLAN by entering this command in VLAN configuration mode.

Examples

This example shows how to limit Internet Group Management Protocol (IGMP) traffic sent from all interfaces in the Virtual Supervisor Module (VSM):

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip igmp snooping link-local-groups-suppression
n1000v(config)#
```

This example shows how to resume sending unlimited IGMP traffic from all interfaces in the VSM:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no ip igmp snooping link-local-groups-suppression
n1000v(config)#
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on a VLAN.
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping mrouter interface

To configure a static connection to a multicast router, use the **ip igmp snooping mrouter interface** command. To remove the static connection, use the **no** form of this command.

ip igmp snooping mrouter interface *if-type if-number*

no ip igmp snooping mrouter interface *if-type if-number*

Syntax Description

if-type	Specifies interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. The values vary by interface. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Defaults

None

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Usage Guidelines

The interface to the router must be in the selected VLAN.

Examples

This example shows how to configure a static connection to a multicast router:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)#
```

This example shows how to remove a static connection to a multicast router:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# no ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays Internet Group Management Protocol (IGMP) snooping information.

ip igmp snooping report-suppression (Global)

To configure Internet Group Management Protocol Version 1 (IGMPv1) or IGMPv2 report suppression for VLANs, use the **ip igmp snooping report-suppression** command. To remove IGMPv1 or IGMPv2 report suppression, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Examples

This example shows how to configure IGMPv1 or IGMPv2 report suppression for VLANs:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip igmp snooping report-suppression
```

This example shows how to remove IGMPv1 or IGMPv2 report suppression:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no ip igmp snooping report-suppression
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping report-suppression (VLAN)

To configure Internet Group Management Protocol Version 1 (IGMPv1) or IGMPv2 report suppression for VLANs, use the **ip igmp snooping report-suppression** command. To remove IGMPv1 or IGMPv2 report suppression, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Examples

This example shows how to configure IGMPv1 or IGMPv2 report suppression for VLAN 342:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping report-suppression
n1000v(config-vlan)#
```

This example shows how to remove IGMPv1 or IGMPv2 report suppression from VLAN 342:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# no ip igmp snooping report-suppression
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping static-group

To configure a Layer 2 port of a VLAN as a static member of a multicast group, use the **ip igmp snooping static-group** command. To remove the static member, use the **no** form of this command.

ip igmp snooping static-group *group* **interface** *if-type if-number*

no ip igmp snooping static-group *group* **interface** *if-type if-number*

Syntax Description

group	Group IP address.
interface	Specifies the interface for a static group.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Defaults

None

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Usage Guidelines

You can specify the interface by the type and the number, such as ethernet slot/port.

Examples

This example shows how to configure a static member of a multicast group:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
n1000v(config-vlan)#
```

This example shows how to remove a static member of a multicast group:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# no ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping v3-report-suppression (Global)

To configure Internet Group Management Protocol Version 3 (IGMPv3) report suppression and proxy reporting, use the **ip igmp snooping v3-report-suppression** command. To remove IGMPv3 report suppression and proxy reporting, use the **no** form of this command.

ip igmp snooping v3-report-suppression

no ip igmp snooping v3-report-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Examples

This example shows how to configure IGMPv3 report suppression and proxy reporting:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip igmp snooping v3-report-suppression
```

This example shows how to remove IGMPv3 report suppression and proxy reporting:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no ip igmp snooping v3-report-suppression
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping v3-report-suppression (VLAN)

To configure Internet Group Management Protocol Version 3 (IGMPv3) report suppression and proxy reporting for a VLAN, use the **ip igmp snooping v3-report-suppression** command. To remove IGMPv3 report suppression, use the **no** form of this command.

ip igmp snooping v3-report-suppression

no ip igmp snooping v3-report-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Examples

This example shows how to configure IGMPv3 report suppression and proxy reporting for VLAN 342:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# ip igmp snooping v3-report-suppression
n1000v(config-vlan)#
```

This example shows how to remove IGMPv3 report suppression and proxy reporting for VLAN 342:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# vlan configuration 342
n1000v(config-vlan)# no ip igmp snooping v3-report-suppression
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip port access-group

To create an access group, use the **ip port access-group** command. To remove access control, use the **no** form of this command.

ip port access-group *name* {**in** | **out**}

no ip port access-group *name* {**in** | **out**}

Syntax Description

name	Access group name. The range is from 1 to 64, case-sensitive, alphanumeric characters.
in	Specifies inbound traffic.
out	Specifies outbound traffic.

Defaults

No access group exists.

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Usage Guidelines

You create an access group to specify in an access control list (ACL) the access control of packets.

Examples

This example shows how to create an access group:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-profile 1
n1000v(config-port-prof)# ip port access-group group1 in
n1000v(config-port-prof)#
```

Related Commands

Command	Description
show access-lists	Displays access lists.
show port-profile	Displays port profile information.

ip prec

To specify the IP precedence value for the packets in the Encapsulated Remote Switch Port Analyzer (ERSPAN) traffic and save it in the running configuration, use the **ip prec** command.

ip prec *precedence_value*

Syntax Description

precedence_value	IP precedence value for the ERSPAN traffic packets. The range is from 0 to 7.

Defaults

None

Command Modes

Command-line interface (CLI) ERSPAN source configuration (config-monitor-erspan-src)

SupportedUserRoles

network-admin

Examples

This example shows how to specify the IP precedence value as 1 for the packets in the ERSPAN traffic and save it in the running configuration:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# destination ip 10.54.54.1
n1000v(config-monitor-erspan-src)# ip prec 1
n1000v(config-monitor-erspan-src)#
```

Related Commands

Command	Description
description	For the specified ERSPAN session, adds a description and saves it in the running configuration.
destination ip	Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration.
erspan-id	Adds an ERSPAN ID to the session configuration and saves it in the running configuration.
filter vlan	Configures the VLANs, VLAN lists, or VLAN ranges to be monitored for the specified session; and saves this information in the running configuration.
ip dscp	Specifies the IP DSCP value for the packets in the ERSPAN traffic, and saves it in the running configuration.
ip ttl	Specifies the IP time-to-live value for the packets in the ERSPAN traffic, and saves it in the running configuration.
monitor session type erspan-source	Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode.
no shut	Enables the ERSPAN session and saves it in the running configuration.

Command	Description
show monitor session session_id	Displays the ERSPAN session configuration as it exists in the running configuration.
source	Configures the sources and the direction of traffic to monitor for the specified session, and saves the information in the running configuration.

ip source binding

To create a static IP source entry for a Layer 2 virtual Ethernet interface, use the **ip source binding** command. To disable the static IP source entry, use the **no** form of this command.

ip source binding *IP-address MAC-address* **vlan** *vlan-id* **interface vethernet** *interface-number*

no ip source binding *IP-address MAC-address* **vlan** *vlan-id* **interface vethernet** *interface-number*

Syntax Description

IP-address	IPv4 address to be used on the specified interface. Valid entries are in dotted-decimal format.
MAC-address	MAC address to be used on the specified interface. Valid entries are in dotted-hexadecimal format.
vlan	Specifies the VLAN associated with the IP source entry.
vlan-id	VLAN number. The range is from 1 to 4096.
interface vethernet	Specifies the Layer 2 virtual Ethernet interface that is associated with the static IP entry.
interface-number	Virtual Ethernet number. The range is from 1 to 1048575.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Usage Guidelines

By default, there are no static IP source entries.

Examples

This example shows how to create a static IP source entry that is associated with VLAN 100 on virtual Ethernet interface 3:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface vethernet 3
n1000v(config)#
```

Related Commands

Command	Description
ip verify source dhcp-snooping-vlan	Enables IP Source Guard on an interface.
show ip verify source	Displays IP-to-MAC address bindings.

ip ttl

To specify the IP time-to-live value for the packets in the Encapsulated Remote Switch Port Analyzer (ERSPAN) traffic and save it in the running configuration, use the **ip ttl** command.

ip ttl *ttl_value*

Syntax Description

ttl_value	Time-to-live value, in seconds. The range is from 1 to 255.

Defaults

None

Command Modes

Command-line interface (CLI) ERSPAN source configuration (config-monitor-erspan-src)

SupportedUserRoles

network-admin

Examples

This example shows how to specify the time-to-live value of 64 seconds for packets in the ERSPAN traffic:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# destination ip 10.54.54.1
nn1000v(config-erspan-src)# ip ttl 64
n1000v(config-erspan-src)#
```

Related Commands

Command	Description
description	For the specified ERSPAN session, adds a description and saves it in the running configuration.
destination ip	Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration.
erspan-id	Adds an ERSPAN ID to the session configuration and saves it in the running configuration.
filter vlan	Configures the VLANs, VLAN lists, or VLAN ranges to be monitored for the specified session; and saves this information in the running configuration.
ip dscp	Specifies the IP DSCP value for the packets in the ERSPAN traffic, and saves it in the running configuration.
ip prec	Specifies the IP precedence value for the packets in the ERSPAN traffic, and saves it in the running configuration.
monitor session type erspan-source	Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode.
no shut	Enables the ERSPAN session and saves it in the running configuration.

Command	Description
show monitor session session_id	Displays the ERSPAN session configuration as it exists in the running configuration.
source	Configures the sources and the direction of traffic to monitor for the specified session, and saves the information in the running configuration.

ip verify source dhcp-snooping-vlan

To enable IP Source Guard on a Layer 2 virtual Ethernet interface, use the **ip verify source dhcp-snooping-vlan** command. To disable IP Source Guard (SG) on an interface, use the **no** form of this command. To restore the default setting, use the **default** form of this command.

ip verify source dhcp-snooping-vlan

no ip verify source dhcp-snooping-vlan

default ip verify source dhcp-snooping-vlan

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Usage Guidelines

By default, IP Source Guard is not enabled on any interface.

Examples

This example shows how to enable IP SG on an interface:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip verify source dhcp-snooping-vlan
n1000v(config-if)#
```

Related Commands

Command	Description
ip source binding	Creates a static IP source entry for the specified virtual Ethernet interface.
show ip verify source	Displays IP-to-MAC address bindings.