I Commands

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

id

To associate a network segmentation policy with the tenant ID, use the **id** command.

id *isolation_id*

Syntax Description

isolation_id	The tenant ID of the network segmentation policy.

Defaults

None

Command Modes

Network Segment Policy configuration (config-network-segment-policy)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(5.1)	This command was introduced.

Usage Guidelines

The tenant ID correlates to the Organization UUID in the vCloud Director and cannot be changed once it is configured.

Examples

This example shows how associate a network segmentation policy with the tenant ID:

```
n1000v# configure terminal
n1000v(config)# network-segment policy abc-policy-vxlan
n1000v(config-network-segment-policy)#id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
```

Related Commands

Command	Description
network-segment policy	Creates a network segmentation policy.
show run network-segment policy	Displays the network segmentation policy configuration.

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	Name for the port profile whose policies are inherited. The name can be up to 80 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Any inherited setting, except the port profile type, can be changed using the CLI.

When you use the **no** form of the 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# config t
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# config t
n1000v(config)# port-profile type vethernet AllAccess2
n1000v(config-port-prof)# no port-profile inherit
```

Related Commands

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

install certificate

To install a certificate, use the **install certificate** command. To remove a certificate, use the **no** form of this command.

install certificate {**bootflash:** | **default**}

no install certificate

Syntax Description

bootflash:	Specifies the path.
default	Specifies the default certificate.

Defaults

No certificate is installed.

Command Modes

SVS connection configuration (config-svs-conn)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Only one SVS connection can be created.

Examples

This example shows how to install a certificate:

```
n1000v# configure terminal
n1000v(config)# svs connect s1
n1000v(config-svs-conn)# install certificate default
n1000v(config-svs-conn)#
```

This example shows how to remove a certificate:

```
n1000v# configure terminal
n1000v(config)# svs connect s1
n1000v(config-svs-conn)# no install certificate default
n1000v(config-svs-conn)#
```

Related Commands

Command	Description
show svs	Displays SVS information.

install http certificate

To change the security certificate for the HTTP server, use the **install http certificate bootflash:<cert_path>** command. To remove the security certificate, use the **no** form of this command.

install http certificate {**bootflash: | default**}

no install http certificate

Syntax Description

bootflash:	Specifies the path.
default	Specifies the default certificate.

Defaults

No HTTP certificate is installed.

Command Modes

SVS connection configuration (config-svs-conn)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Only one SVS connection can be created.

Examples

This example shows how to install a HTTP certificate:

```
n1000v# configure terminal
n1000v(config)# svs connect s1
n1000v(config-svs-conn)# install http certificate bootflash:<cert_path>
n1000v(config-svs-conn)#
```

This example shows how to remove a HTTP certificate:

```
n1000v# configure terminal
n1000v(config)# svs connect s1
n1000v(config-svs-conn)# no install http certificate bootflash:<cert_path>
n1000v(config-svs-conn)#
```

Related Commands

Command	Description
show svs	Displays SVS information.

install license bootflash:

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

install license bootflash: *filename*

Syntax Description

filename	(Optional) Specify a name for the license file. If you do not specify a name, then the license is installed using the default name.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

- You must first uninstall an evaluation license if one is present on your VSM. For more information, see the *Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)*.
- 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 file name 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
show license file	Verifies the license installation by displaying the license configured for the VSM.
clear license	Uninstalls a license, that is, removes it from the VSM and shuts down the Ethernet interfaces to the VEMs covered by that license.
logging level license	Designates the level of severity at which license messages should be logged.
install license	Installs a license file(s) on a VSM
svs license transfer src-vem	Transfers licenses from a source VEM to another VEM, or to the VSM pool of available licenses.

install service-module (kickstart and system image)

To upgrade a VXLAN gateway service module (standalone) or a VXLAN gateway high availability (HA) cluster by using the kickstart and the system images, use the **install service-module** command.

install service-module kickstart bootflash: *kickstart_image* **system bootflash:** *system_image* {**module-num** *module_number* | **cluster-id** *cluster_id*}

Syntax Description

kickstart_image	Name of the kickstart image.
system_image	Name of the system image.
module_number	The module number. The module number range is from 3 to 130.
cluster_id	The cluster ID. The cluster ID range is from 1 to 8.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.2(1)SV2(2.1a)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to upgrade a VXLAN gateway cluster:

```
n1000v# install service-module kickstart
bootflash:vxgw-kickstart-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg system
bootflash:vxgw-1000v-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg cluster-id 1

Verifying image bootflash:/vxgw-kickstart-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg for boot
variable "kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/vxgw-1000v-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg for boot
variable "system".
[####################] 100% -- SUCCESS
Output commands:
----------------
Extracting SRG from the Service Module image
bootflash:/vxgw-1000v-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg.
[####################] 100% -- SUCCESS

Service Module compatibility check is done:
```

```
   VSM Version    Service Module Version  Compatible
---------------  ----------------------  ----------
 4.2(1)SV2(2.1a)     4.2(1u)SV2(2.1au)        yes

Do you want to continue with the Service Module installation (y/n)?  [n] y

Install is in progress, please wait.

Copying bootflash:/vxgw-kickstart-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg to Service Module
10.105.234.177.
[####################] 100% -- SUCCESS

Copying bootflash:/vxgw-1000v-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg to Service Module
10.105.234.177.
[####################] 100% -- SUCCESS

Copying bootflash:/vxgw-kickstart-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg to Service Module
10.105.234.176.
[####################] 100% -- SUCCESS

Copying bootflash:/vxgw-1000v-upgrade.4.2.1.SV2.1a.2.0.315.bin.upg to Service Module
10.105.234.176.
[####################] 100% -- SUCCESS

Set bootvariables on the standby Service Module.

Sent reboot message to standby Service Module.
```

Related Commands

Command	Description
install service-module (iso image)	Upgrades a VXLAN gateway service module (standalone) or a VXLAN gateway high availability (HA) cluster by using the iso image.
show module service-module	Displays Cluster-id, HA-role, HA mode, and HA-status for service modules attached to the VSM.

install service-module (iso image)

To upgrade a VXLAN gateway service module (standalone) or a VXLAN gateway high availability (HA) cluster by using the iso image, use the **install service-module** command.

install service-module iso bootflash: *iso_image* {**module-num** *module_number* | **cluster-id** *cluster_id*}

Syntax Description

iso_image	Name of the iso image.
module_number	The module number. The module number range is from 3 to 130.
cluster_id	The cluster ID. The cluster ID range is from 1 to 8.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.2(1)SV2(2.1a)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to upgrade a VXLAN gateway cluster:

```
n1000v# install service-module iso bootflash:vxgw.4.2.1.SV2.2.2.iso cluster-id 1

Verifying image bootflash:/vxgw-kickstart.4.2.1.SV2.2.2.gbin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/vxgw.4.2.1.SV2.2.2.gbin for boot variable "system".
[####################] 100% -- SUCCESS

Extracting SRG from the Service Module image bootflash:/vxgw.4.2.1.SV2.2.2.gbin.
[####################] 100% -- SUCCESS

Service Module compatibility check is done:
   VSM Version    Service Module Version  Compatible
---------------  ----------------------  ----------
  4.2(1)SV2(2.2)       4.2(1)SV2(2.2)        yes

Do you want to continue with the Service Module installation (y/n)?  [n] y
```

```
Install is in progress, please wait.

Copying bootflash:/vxgw-kickstart.4.2.1.SV2.2.2.gbin to Service Module 10.105.232.77.
[####################] 100% -- SUCCESS

Copying bootflash:/vxgw.4.2.1.SV2.2.2.gbin to Service Module 10.105.232.77.
[####################] 100% -- SUCCESS

Copying bootflash:/vxgw-kickstart.4.2.1.SV2.2.2.gbin to Service Module 10.105.232.202.
[####################] 100% -- SUCCESS

Copying bootflash:/vxgw.4.2.1.SV2.2.2.gbin to Service Module 10.105.232.202.
[####################] 100% -- SUCCESS

Set bootvariables on the standby Service Module.

Sent reboot message to standby Service Module.
2014 Jan 15 07:02:34 CY %VEM_MGR-2-VEM_MGR_REMOVE_NO_HB: Removing VEM 9 (heartbeats lost)
2014 Jan 15 07:02:35 CY %VEM_MGR-2-MOD_OFFLINE: Module 9 is offline
```

Related Commands

Command	Description
install service-module (kickstart and system image)	Upgrades a VXLAN gateway service module (standalone) or a VXLAN gateway high availability (HA) cluster by using the kickstart and the system image.
show module service-module	Displays Cluster-id, HA-role, HA mode, and HA-status for service modules attached to the VSM.

interface control

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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines None

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

```
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	Specifies the slot number and port number for the Ethernet interface.

Defaults

None

Command Modes

Global configuration (config)

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Examples

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

```
n1000v# config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)#
```

Related Commands

Command	Description
show interface ethernet *slot/port*	Displays information about the Ethernet interface.

interface loopback

To create and configure a loopback interface, use the **interface loopback** command. To remove a loopback interface, use the **no** form of this command.

interface loopback *number*

no interface loopback *number*

Syntax Description

number	Identifying interface number; valid values are from 0 to 1023.

Defaults

None

Command Modes

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

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Examples

This example shows how to create a loopback interface:

```
n1000v(config)# interface loopback 50
n1000v(config-if)#
```

Related Commands

Command	Description
show interface loopback	Displays information about the traffic on the specified loopback interface.

interface mgmt

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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Examples

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

```
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 of valid values is from 1 to 4096.

Defaults

None

Command Modes

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

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Use the **interface port-channel** command to create or delete port-channel groups and to enter the 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 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(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 on 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	Identifying interface number; valid values are from 1 to 1048575.

Defaults

None

Command Modes

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

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

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(config)# interface vethernet 50
n1000v(config-if)#
```

Related Commands

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

ip access-group

To create an IP access group for 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.
in	Specify incoming (ingress) traffic direction.
out	Specify outgoing (egress) traffic direction.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1) SV1(4)	This command was introduced.

Usage Guidelines

Examples

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

```
n1000v# config t
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.
match-local-traffic	Enables access list matching for locally generated traffic.

Defaults

No access list exists.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to create an access list:

```
n1000v# configure terminal
n1000v(config)# ip access-list acl1
n1000v(config)#
```

Related Commands

Command	Description
show access-lists	Displays access lists.

ip address

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

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

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

Syntax Description

address	IP address, in format A.B.C.D.
mask	IP network mask, in format A.B.C.D.
prefix	IP prefix and network mask length, in format A.B.C.D/LEN.
next-hop	IP next-hop address, in format A.B.C.D.
next-hop-prefix	IP next-hop prefix in format A.B.C.D./LEN.
interface-type	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 of valid values is 0 to 4294967295. The default is 0.
preference	(Optional) Route preference.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to create an IP address:

```
n1000v# configure terminal
n1000v(config)# ip address 209.165.200.225 255.255.255.224 x
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 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

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

Examples

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

```
n1000v(config)# ip arp inspection limit rate 20
```

This example shows how to remove the configuration:

```
n1000v(config)# no arp inspection limit rate 20
```

Related Commands

Command	Description
show ip arp inspection interface 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 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

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

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
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 ARP Inspection (DAI) validation, use the **ip arp inspection validate** command. To disable additional DAI, 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

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

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
n1000v(config)# ip arp inspection validate src-mac dst-mac ip
n1000v(config)#
```

Related Commands

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

ip arp inspection vlan

To enable Dynamic 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 ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

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
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 DHCP snooping on the device, 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

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

Usage Guidelines

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

The device preserves 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
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 VSM MAC address and vEthernet port information in 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

Command History

Release	Modification
4.2(1)SV1(4)	This command was introduced.

Usage Guidelines

Examples

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

```
n1000v# configure terminal
n1000v(config)# ip dhcp snooping information option
n1000v(config)#
```

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

```
n1000v# configure terminal
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 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	Number of 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

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

Examples

This example shows how to limit the rate of DHCP packets to 30 pps on vEthernet interface 3:

```
n1000v# configure terminal
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 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

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

Usage Guidelines

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

- Layer 2 vEthernet interfaces
- Private VLAN interfaces

Examples

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

```
n1000v# configure terminal
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.

Command	Description
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 DHCP snooping 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v(config)# config t
n1000v(config)# ip dhcp snooping verify mac-address
n1000v(config)#
```

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

```
n1000v(config)# config t
n1000v(config)# no ip dhcp snooping verify mac-address
n1000v(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
show running-config dhcp	Displays the DHCP snooping configuration.
ip dhcp snooping	Enables DHCP snooping globally.
ip dhcp snooping vlan	Enables DHCP snooping on the VLANs specified by *vlan-list*.
clear ip dhcp snooping binding	Clears dynamically added entries from the DHCP snooping binding database.

Command	Description
ip dhcp snooping trust	Configures the interface as a trusted interface for DHCP snooping.
ip dhcp snooping limit rate	Configures the DHCP limit rate.

ip dhcp snooping vlan

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

Defaults

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

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

Examples

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

```
n1000v# configure terminal
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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to enable IP directed broadcast:

```
n1000v# configure terminal
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 DSCP value for the packets in the 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 value can range from 0–63.

Defaults

The default DSCP value is 0.

Command Modes

CLI ERSPAN source configuration (config-erspan-src)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# ip dscp 25
n1000v(config-erspan-src)#
```

Related Commands

Command	Description
monitor session type erspan-source	Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode.
description	For the specified ERSPAN session, adds a description and saves it 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.
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.
destination ip	Configures the IP address of the host to which the encapsulated traffic is sent 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.

Command	Description
ip prec	Specifies the IP precedence value for the packets in the ERSPAN traffic, and saves it in the running configuration.
mtu	Specifies a maximum transmission unit (MTU) size for the ERSPAN traffic, and saves it in the running configuration.
erspan-id	Adds an ERSPAN ID to the session configuration and saves it in the running configuration.
no shut	Enables the ERSPAN session and saves it in the running configuration.
show monitor session *session_id*	Displays the ERSPAN session configuration as it exists 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** interface configuration mode 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	Name of a flow monitor that you previously configured.
input	Monitors traffic that the routers is receiving on the interface.
output	Monitors traffic that the routers is transmitting on the interface.

Defaults

Disabled.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

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

The following example enables a flow monitor for monitoring input traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring output traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

The following example enables the same flow monitor on the same interface for monitoring input and output traffic:

```
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
```

The following example enables two different flow monitors on the same interface for monitoring input and output traffic:

```
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
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output traffic:

```
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
```

The following example enables two different flow monitors on two different interfaces for monitoring input and output traffic:

```
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 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to enable IGMP snooping:

```
n1000v(config)# ip igmp snooping
n1000v(config)#
```

This example shows how to disable IGMP snooping:

```
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 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

If the global configuration of IGMP snooping is disabled, then 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(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping
n1000v(config-vlan)#
```

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

```
n1000v(config)# vlan 1
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 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 configuration (config-vlan)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping explicit-tracking
n1000v(config-vlan)#
```

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

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping explicit-tracking
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping fast-leave

To enable support of 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port.

Examples

This example shows how to enable support of IGMPv2 hosts:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping fast-leave
n1000v(config-vlan)#
```

This example shows how to disable support of IGMPv2 hosts:

```
n1000v(config)# vlan 1
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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v(config)# vlan 1
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(config)# vlan 1
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 IPs, 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

Command History

Release	Modification
4.2(1) SV1(4)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to limit IGMP traffic sent from VLAN2:

```
n1000v# config t
n1000v(config)# vlan vlan2
n1000v(config-vlan)# ip igmp snooping link-local-groups-suppression
```

This example shows how to resume IGMP traffic sent from VLAN2:

```
n1000v# config t
n1000v(config)# vlan vlan2
n1000v(config-vlan)# no ip igmp snooping link-local-groups-suppression
n1000v(config-vlan)#
```

Related Commands

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

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

To suppress snooping on link-local group IPs, 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

Command History

Release	Modification
4.2(1) SV1(4)	This command was introduced.

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 IGMP traffic sent from all interfaces in the VSM:

```
n1000v# config t
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# config t
n1000v(config)# no ip igmp snooping link-local-groups-suppression
n1000v(config)#
```

Related Commands

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

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	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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

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(config)# vlan 1
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(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping report-suppression (Global)

To configure IGMPv1 or GMPv2 report suppression for VLANs, use the **ip igmp snooping report-suppression** command. To remove IGMPv1 or GMPv2 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to configure IGMPv1 or GMPv2 report suppression for VLANs:

```
n1000v(config)# ip igmp snooping report-suppression
```

This example shows how to remove IGMPv1 or GMPv2 report suppression:

```
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 IGMPv1 or GMPv2 report suppression for VLANs, use the **ip igmp snooping report-suppression** command. To remove IGMPv1 or GMPv2 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to configure IGMPv1 or GMPv2 report suppression for VLANs:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping report-suppression
n1000v(config-vlan)#
```

This example shows how to remove IGMPv1 or GMPv2 report suppression:

```
n1000v(config)# vlan 1
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 interface for 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

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(config)# vlan 1
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(config)# vlan 1
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 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v(config)# ip igmp snooping v3-report-suppression
```

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

```
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 IGMPv3 report suppression and proxy reporting for VLANs, 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

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v(config)# vlan 1
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 VLANs:

```
n1000v(config)# vlan 1
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	Group name. The range of valid values is 1 to 64.
in	Specifies inbound traffic.
out	Specifies outbound traffic.

Defaults

No access group exists.

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to create an access group:

```
n1000v# configure terminal
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 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 0–7.

Defaults

None

Command Modes

CLI ERSPAN source configuration (config-monitor-erspan-src)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

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# config t
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
monitor session type erspan-source	Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode.
description	For the specified ERSPAN session, adds a description and saves it 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.
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.
destination ip	Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration.

Command	Description
ip ttl	Specifies the IP time-to-live value for the packets in the ERSPAN traffic, and saves it 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.
mtu	Specifies a maximum transmission unit (MTU) size for the ERSPAN traffic, and saves it in the running configuration.
erspan-id	Adds an ERSPAN ID to the session configuration and saves it in the running configuration.
no shut	Enables the ERSPAN session and saves it in the running configuration.
show monitor session session_id	Displays the ERSPAN session configuration as it exists in the running configuration.

ip source binding

To create a static IP source entry for a Layer 2 vEthernet 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 *vlan-id*	Specifies the VLAN associated with the IP source entry.
interface vethernet *interface-number*	Specifies the Layer 2 vEthernet interface associated with the static IP entry.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

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 vEthernet interface 3:

```
n1000v# configure terminal
n1000v(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface vethernet 3
n1000v(config)#
```

Related Commands

Command	Description
show ip dhcp snooping binding	Displays IP-to-MAC address bindings.

ip source binding filter-mode [*ip* | *ip-mac*]

Use the **ip source binding** [*ip* | *ip-mac*]command to enable source IP based filtering.

ip source binding *filter-mode* [*ip* | *ip-mac*]

Syntax Description

filter-mode	Filter mode to be used on the switch. The available filter modes are *ip* and *ip-mac*. Use the *ip* filter mode to filter the traffic based on the source IP address. Use the *ip-mac* filter mode to filter the traffic based on the IP-MAC Address pair.

Defaults

ip-mac

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2.1SV2(1.1)	This command was introduced to include the ip filter mode.

Usage Guidelines

This functionality is applicable to static bindings only. In the case of the dynamic bindings, a new MAC Address results in updating the dynamic binding on the Cisco Nexus 1000V.

Examples

This example shows how to enable source-IP only filtering for IPSG/DAI:

```
n1000v# configure terminal
n1000v(config)# ip source binding filter-mode ip
n1000v(config)#
```

Related Commands

Command	Description
show ip source binding filter-mode	Displays IP-to-MAC address bindings and the filter mode.
show ip arp inspection	Displays IP-to-MAC address bindings and the filter mode.
show ip verify source	Displays IP-to-MAC address bindings and the filter mode.

ip source-route

To enable an IP source route, use the **ip source-route** command. To disable an IP source route, use the **no** form of this command.

ip source-route

no ip source-route

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to enable an IP source route:

```
n1000v# configure terminal
n1000v(config)# ip source-route
n1000v(config)#
```

Related Commands

Command	Description
show ip static-route	Displays static routes.

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, from 1–255.

Defaults

None

Command Modes

CLI ERSPAN source configuration (config-monitor-erspan-src)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

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

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# destination ip 10.54.54.1
nn1000v(config-monitor-erspan-src)# ip ttl 64
n1000v(config-monitor-erspan-src)#
```

Related Commands

Command	Description
monitor session type erspan-source	Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode.
description	For the specified ERSPAN session, adds a description and saves it 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.
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.
destination ip	Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration.

Command	Description
ip prec	Specifies the IP precedence value for the packets in the ERSPAN traffic, and saves it 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.
mtu	Specifies a maximum transmission unit (MTU) size for the ERSPAN traffic, and saves it in the running configuration.
erspan-id	Adds an ERSPAN ID to the session configuration and saves it in the running configuration.
no shut	Enables the ERSPAN session and saves it in the running configuration.
show monitor session session_id	Displays the ERSPAN session configuration as it exists in the running configuration.

ip verify source dhcp-snooping-vlan

To enable IP Source Guard on a Layer 2 vEthernet interface, use the **ip verify source dhcp-snooping-vlan** command. To disable IP Source Guard 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

Command History

Release	Modification
4.0(4)SV1(2)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to enable IP Source Guard on an interface:

```
n1000v# configure terminal
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 vEthernet interface.
show ip verify source	Displays IP-to-MAC address bindings.