C Commands

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

cache size

To specify a cache size for a Netflow flow monitor, use the **cache size** command. To remove the cache size for a flow monitor, use the **no** form of this command.

cache size *value*

no cache size *value*

Syntax Description

value	Size in number of entries. The range is 256 to 16384 entries.

Defaults

4096 entries

Command Modes

Netflow monitor configuration (**config-flow-monitor**)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use the **cache-size** command to limit the impact of the Netflow flow monitor cache on memory and performance.

Examples

This example shows how to configure the cache size for a Netflow flow monitor named MonitorTest, and then display the configuration:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# cache size 15000
n1000v(config-flow-monitor)# show flow monitor MonitorTestFlow
Monitor monitortest:
     Use count: 0
     Inactive timeout: 600
     Active timeout: 1800
     Cache Size: 15000
n1000v(config-flow-monitor)#
```

This example shows how to remove a cache size from a flow monitor:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# no cache size
n1000v(config-flow-monitor)#show flow monitor MonitorTestFlow
n1000v(config-flow-monitor)#
Monitor monitortest:
     Use count: 0
     Inactive timeout: 600
     Active timeout: 1800
     Cache Size: 4096
n1000v(config-flow-monitor)#
```

Related Commands

Command	Description
show flow monitor	Displays information about the flow monitor cache module.
flow monitor	Creates a flow monitor.
timeout	Specifies an aging timer and its value for aging entries from the cache.
record	Adds a flow record to the flow monitor.
exporter	Adds a flow exporter to the flow monitor.

capability iscsi-multipath

To configure a port profile to be used with the ISCSI Multipath protocol, use the **capability iscsi-multipath** command. To remove the capability from a port profile, use the **no** form of this command.

capability iscsi-multipath

no capability iscsi-multipath

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(2)	Added the **capability iscsi multipath** command.

Usage Guidelines

If you are configuring a port profile for ISCSI Multipath, then you must first configure the port profile in switchport mode.

Examples

This example shows how to configure a port profile to be used with ISCSI Multipath protocol:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# switchport mode access
n1000v(config-port-prof)# capability iscsi-multipath
n1000v(config-port-prof)#
```

This example shows how to remove the ISCSI multipath configuration from the port profile:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# no capability iscsi-multipath
n1000v(config-port-prof)#
```

Related Commands

Command	Description
show port-profile name [*name*]	Displays the port profile configuration.
port-profile *name*	Places you into port profile configuration mode for creating and configuring a port profile.

capability l3control

To configure the Layer 3 capability for a port profile, use the **capability** command. To remove a capability from a port profile, use the **no** form of this command.

capability l3control

no capability l3control

Syntax Description

l3control	Configures a port profile to be used for one of the following Layer 3 communication purposes: • The management interface used for Layer 3 communication between the VSM and VEMs. • To carry NetFlow ERSPAN traffic.

Defaults

None

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	Introduced the **capability uplink** command to designate a port profile as an uplink.
4.0(4)SV1(2)	Removed the **capability uplink** command. A port profile used as an uplink is now designated as type Ethernet instead. Added the **capability l3control** command.

Usage Guidelines

If you are configuring a port profile for Layer 3 control, then you must first configure the transport mode as Layer 3 using the **svs mode** command for the VSM domain.

Examples

This example shows how to configure a port profile to be used for Layer 3 communication purposes:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# capability l3control
n1000v(config-port-prof)#
```

This example shows how to remove the Layer 3 configuration from the port profile:

```
n1000v# config t
```

```
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# no capability l3control
n1000v(config-port-prof)#
```

Related Commands

Command	Description
show port-profile name [*name*]	Displays the port profile configuration.
port-profile *name*	Places you into port profile configuration mode for creating and configuring a port profile.

capability vxlan

To assign the VXLAN capability to the port profile to ensure that the interfaces that inherit this port profile are used as sources for VXLAN encapsulated traffic, use the **capability vxlan** command. To remove the VXLAN capability, use the **no** form of this command.

capability vxlan

no capability vxlan

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to assign the VXLAN capability to port profile vmnic-pp:

```
n1000v# configure terminal
n1000v(config)# port-profile vmknic-pp
n1000v(config-port-prof)# capability vxlan
n1000v(config-port-prof)
```

Related Commands

Command	Description
show bridge-domain	Displays bridge domain information.
show interface virtual	Displays information about virtual interfaces.
show running config interface vethernet	Displays information about the running configuration of the vEthernet interface.
show port-profile usage	Display the usage for all port profiles.

cd

To change to a different directory from the one you are currently working in, use the **cd** command.

cd [*filesystem*:[*//directory*] | *directory*]

Syntax Description

filesystem:	(Optional) Name of the file system. Valid file systems are **bootflash** and **volatile**.
//directory	(Optional) Name of the directory. The directory name is case sensitive.

Defaults

bootflash

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

You can only change to the directories that are on the active supervisor module.

Use the present working directory (**pwd**) command to verify the name of the directory you are currently working in.

Examples

This example shows how to change to a different directory on the current file system:

```
n1000v# cd my-scripts
```

This example shows how to change from the file system you are currently working in to a different file system:

```
n1000v# cd volatile:
```

This example shows how to revert back to the default directory, bootflash:

```
n1000v# cd
```

Related Commands

Command	Description
pwd	Displays the name of the directory you are currently working in.

cdp advertise

To specify the CDP version to advertise, use the **cdp advertise** command. To remove the cdp advertise configuration, use the **no** form of this command.

cdp advertise {**v1** | **v2**}

no cdp advertise [**v1** | **v2**]

Syntax Description

v1	CDP Version 1.
v2	CDP Version 2.

Defaults

CDP Version 2

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 set CDP Version 1 as the version to advertise:

```
n1000v(config)# cdp advertise v1
```

This example shows how to remove CDP Version 1 as the configuration to advertise:

```
n1000v(config)# no cdp advertise v1
```

Related Commands

Command	Description
show cdp global	Displays the CDP configuration.

cdp enable (global)

To enable Cisco Discovery Protocol (CDP) globally on all interfaces and port channels, use the **cdp enable** command. To disable CDP globally, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled on all interfaces and port channels

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

CDP can only be configured on physical interfaces and port channels.

Examples

This example shows how to enable CDP globally and then show the CDP configuration:

```
n1000v# config t
n1000v(config)# cdp enable
n1000v(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Refresh time is 60 seconds
    Hold time is 180 seconds
    CDPv2 advertisements is enabled
    DeviceID TLV in System-Name(Default) Format
```

This example shows how to disable CDP globally and then show the CDP configuration:

```
n1000v(config)# no cdp enable
n1000v# show cdp global
Global CDP information:
    CDP disabled globally
    Refresh time is 60 seconds
    Hold time is 180 seconds
    CDPv2 advertisements is enabled
    DeviceID TLV in System-Name(Default) Format
n1000v(config)#
```

Related Commands

Command	Description
show cdp global	Displays the CDP configuration.
cdp enable (interface or port channel)	Enables CDP on an interface or port channel.

cdp enable (interface or port channel)

To enable Cisco Discovery Protocol (CDP) on an interface or port channel, use the **cdp enable** command. To disable it, use the **no** form of this command.

cdp enable

no cdp enable

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.

Usage Guidelines

CDP can only be configured on physical interfaces and port channels.

Examples

This example shows how to enable CDP on port channel 2:

```
n1000v# config t
n1000v(config)# interface port-channel2
n1000v(config-if)# cdp enable
n1000v(config-if)#
```

This example shows how to disable CDP on mgmt0:

```
n1000v# config t
n1000v(config)# interface mgmt0
n1000v(config-if)# no cdp enable
n1000v(config-if)# show cdp interface mgmt0
        mgmt0 is up
        CDP disabled on interface
        Sending CDP packets every 60 seconds
        Holdtime is 180 seconds
n1000v(config-if)#
```

Related Commands

Command	Description
show cdp interface	Displays the CDP configuration for an interface.
show cdp neighbors	Displays your device from the upstream device.
cdp advertise	Assigns the CPD version the interface will advertise—CDP Version 1 or CDP Version 2.
cdp format device ID	Assigns the CDP device ID
cdp holdtime	Sets the maximum amount of time that CDP holds onto neighbor information before discarding it.

cdp format device-id

To specify the device ID format for CDP, use the **cdp format device-id** command. To remove it, use the **no** form of this command.

cdp format device-id {**mac-address** | **serial-number** | **system-name**}

no cdp format device-id {**mac-address** | **serial-number** | **system-name**}

Syntax Description

mac-address	MAC address of the Chassis.
serial-number	Chassis serial number.
system-name	System name/Fully Qualified Domain Name (Default).

Defaults

System name/Fully Qualified Domain Name

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

CDP must be enabled globally before you configure the device ID format.

You can configure CDP on physical interfaces and port channels only.

Examples

This example shows how to configure the CDP device ID with the MAC address format and then display the configuration:

```
n1000v(config)# cdp format device-id mac-address
n1000v(config)# show cdp global
Global CDP information:
CDP enabled globally
     Sending CDP packets every 5 seconds
     Sending a holdtime value of 10 seconds
     Sending CDPv2 advertisements is disabled
     Sending DeviceID TLV in Mac Address Format
```

This example shows how to remove the CDP device ID MAC address format from the configuration:

```
n1000v(config)# no cdp format device-id mac-address
```

Related Commands

Command	Description
show cdp global	Displays CDP global configuration parameters.
show cdp interface	Displays the CDP configuration for an interface.
show cdp neighbors	Displays your device from the upstream device.
cdp advertise	Assigns the CPD version the interface will advertise—CDP Version 1 or CDP Version 2.
cdp enable interface	Enables CDP on an interface or port channel.
cdp holdtime	Sets the maximum amount of time that CDP holds onto neighbor information before discarding it.

cdp holdtime

To do set the maximum amount of time that CDP holds onto neighbor information before discarding it, use the **cdp holdtime** command. To remove the CDP holdtime configuration, use the **no** form of this command.

cdp holdtime *seconds*

no cdp holdtime *seconds*

Syntax Description

seconds	The range is from 10 to 255 seconds.

Defaults

180 seconds

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

CDP must be enabled globally before you configure the device ID format.

You can configure CDP on physical interfaces and port channels only.

Examples

This example shows how to set the CDP holdtime to 10 second:

```
n1000v(config)# cdp holdtime 10
```

This example shows how to remove the CDP holdtime configuration:

```
n1000v(config)# no cdp holdtime 10
```

Related Commands

Command	Description
show cdp global	Displays CDP global configuration parameters.
show cdp neighbors	Displays the upstream device from your device.

cdp timer

To set the refresh time for CDP to send advertisements to neighbors, use the **cdp timer** command. To remove the CDP timer configuration, use the **no** form of this command.

cdp timer *seconds*

no cdp timer *seconds*

Syntax Description

seconds	The range is from 5 to 254 seconds.

Defaults

60 seconds

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 the CDP timer to 10 seconds:

```
n1000v(config)# cdp timer 10
```

This example shows how to remove the CDP timer configuration:

```
n1000v(config)# no cdp timer 10
```

Related Commands

Command	Description
show cdp global	Displays CDP global configuration parameters.
show cdp neighbors	Displays the upstream device from your device.

channel-group auto (port profile)

To create and define a channel group for all interfaces that belong to a port profile, use the **channel-group auto** command. To remove the channel group, use the **no** form of this command.

channel-group auto [**mode** *channel_mode*] [**sub-group** *sg-type*{**cdp** | **manual**}] [**mac-pinning**]

no channel-group

Syntax Description

mode *channel_mode*	(Optional) Specifies a channeling mode: • **on** • **active** (uses LACP) • **passive** (uses LACP)
sub-group *sg-type*	(Optional) Specifies to create subgroups for managing the traffic flow when the port profile connects to multiple upstream switches. The feature is also called virtual port channel host mode (vPC-HM).
cdp	Specifies to create subgroups using Cisco Discovery Protocol (CDP).
manual	Specifies to create subgroups manually.
mac-pinning	(Optional) Specifies to attach VEMs to an upstream switch that does not support port-channels. There are a maximum of 32 subgroups per port channel, so a maximum of 32 Ethernet port members can be assigned.

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.
4.0(4)SV1(2)	Support for manual creation of subgroups and **mac-pinning**.

Usage Guidelines

The **channel-group auto** command creates a unique port channel for all interfaces that belong to the same module. The channel group is automatically assigned when the port profile is assigned to the first interface. Each additional interface that belongs to the same module is added to the same port channel. In VMware environments, a different port channel is created for each module.

- The channel group mode must be set to **on** when configuring vPC-HM.
- When configuring a port channel for a port profile that connects to two or more upstream switches, note the following:

- You need to know whether CDP is configured in the upstream switches.

  If configured, CDP creates a subgroup for each upstream switch to manage its traffic separately.

  If not configured, then you must manually configure subgroups to manage the traffic flow on the separate switches.
- When configuring a port channel for vPC-HM and the upstream switches do not support port channels, you can use MAC pinning, which will automatically assign each Ethernet member port to a unique sub-group.
- If vPC-HM is not configured when port channels connect to two different upstream switches, the VMs behind the Cisco Nexus 1000V receive duplicate packets from the network for broadcasts and multicasts.
- You can also configure vPC-HM on the interface. For more information, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV2(1.1)*.

Examples

This example shows how to configure a port profile for a port channel that connects to a single upstream switch and then display the configuration:

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# channel-group auto mode on
n1000v(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  status: disabled
  capability uplink: yes
  port-group: AccessProf
  config attributes:
    switchport mode access
    channel-group auto mode on
  evaluated config attributes:
    switchport mode access
    channel-group auto mode on
  assigned interfaces:
n1000v(config-port-prof)#
```

This example shows how to remove the channel group configuration from the port profile and then display the configuration:

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# no channel-group
n1000v(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  status: disabled
  capability uplink: yes
  port-group: AccessProf
  config attributes:
    switchport mode access
evaluated config attributes:
    switchport mode access
assigned interfaces:
n1000v(config-port-prof)#
```

This example shows how to configure a port profile for a port channel that connects to multiple upstream switches that have CDP enabled and then display the configuration:

```
n1000v# config t
n1000v(config)# port-profile uplinkProf
n1000v(config-port-prof)# channel-group auto mode on sub-group cdp
n1000v(config-port-prof)# show port-profile name uplinkProf
port-profile uplinkProf
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group cdp
  evaluated config attributes:
    channel-group auto mode on sub-group cdp
  assigned interfaces:
```

Related Commands

Command	Description
show port-profile name *profile-name*	Displays the port profile configuration.
port-profile *profile-name*	Creates a port profile and places you into global configuration mode for the named port profile.

channel-group (interface)

To create a port channel group or to move an interface from one port channel group to another, use the **channel-group** command. To remove the channel group configuration from an interface, use the **no** form of this command.

channel-group *number* [**force**] [**mode** {**active** | **on** | **passive**}]

no channel-group [*number*]

Syntax Description

number	Number of the channel group. The maximum number of port channels that can be configured is 256. The allowable range of channel group numbers that can be assigned is from 1 to 4096.
force	Forces the interface to join the channel group, although some parameters are not compatible. See Usage Guidelines below for information about the compatibility parameters and which ones can be forced.
mode	Specifies the port channel mode of the interface.
on	This is the default channel mode. All port channels that are not running LACP remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device returns an error message. After you enable LACP globally, you enable LACP on each channel by configuring the channel mode as either active or passive. An interface in this mode does not initiate or respond to LACP packets. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the channel group.
active	Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. Interface is in active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.
passive	Specifies that when you enable LACP, this command enables LACP only if an LACP device is detected.The interface is in a passive negotiation state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.

Defaults

The default mode is **on**.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

A port channel in the **on** channel mode is a pure port channel and can aggregate a maximum of eight ports. It does not run LACP.

If an existing port channel is not running LACP you cannot change the mode for it or any of its interfaces. If you try to do so, the channel mode remains **on** and an error message is generated.

When you delete the last physical interface from a port channel, the port channel remains. To delete the port channel completely, use the **no** form of the **port-channel** command.

When an interface joins a port channel, the following attributes are removed and replaced with the those of the port channel:

- Bandwidth
- Delay
- Extended Authentication Protocol over UDP
- VRF
- IP address
- MAC address
- Spanning Tree Protocol
- NAC
- Service policy
- Quality of Service (QoS)
- ACLs

The following attributes remain unaffected when an interface joins or leaves a port channel:

- Beacon
- Description
- CDP
- LACP port priority
- Debounce
- UDLD
- MDIX
- Rate mode
- Shutdown
- SNMP trap

You do not have to create a port channel interface before you assign a physical interface to a channel group. A port channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

Examples

This example shows how to add an interface to LACP channel group 5 in active mode:

```
n1000v(config-if)# channel-group 5 mode active
n1000v(config-if)#
```

Related Commands

Command	Description
show interface port-channel	Displays information about the traffic on the specified port channel interface.
show port-channel summary	Displays information on the port channels.
feature lacp	Enables the LACP feature globally
show lacp port-channel	Displays LACP information.
show port-channel compatibility-parameters	Displays the list of compatibility checks that the Cisco Nexus 1000V uses.

class (policy map type qos)

To add an existing Quality of Service (QoS) class to a policy map, use the **class** command. To remove a QoS class from a policy map, use the **no** form of this command.

class [**type qos**] {*class-map-name* | **class-default**} [**insert-before** [**type qos**] *before-class-map-name*]

no class {*class-map-name* | **class-default**}

Syntax Description

type qos	(Optional) Specifies the class type to be QoS. QoS is the default class type.
class-map-name	Adds the specified name of an existing class to the policy map.
class-default	Adds the class-default to a policy map. The class-default matches all traffic not classified in other classes.
insert-before *before-class-map-name*	(Optional) Specifies the sequence of this class in the policy by identifying the class map it should precede. If not specified, the class is placed at the end of the list of classes in the policy. Policy actions in the first class that matches the traffic type are performed.

Defaults

type QoS

The default is to reference a new class map at the end of the policy map.

The class named class-default matches all traffic not classified in other classes.

Command Modes

Policy map configuration (config-pmap)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

The class named class-default matches all traffic not classified in other classes.

Examples

This example shows how to add a class map in sequence to the end of a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap)# class traffic_class2
n1000v(config-pmap-c-qos)#
```

This example shows how to insert a class map in sequence before an existing class map in a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap-qos)# class insert-before traffic_class2 traffic_class1
n1000v(config-pmap-c-qos)#
```

This example shows how to add the class-default class map to a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)#
```

This example shows how to remove a class map reference from a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap)# no class traffic_class1
n1000v(config-pmap)#
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map.
set cos	Assigns a CoS to a QoS policy map.
set dscp	Assigns a DSCP value for a traffic class in a QoS policy map.
set precedence	Assigns a precedence value for the IP headers in a specific traffic class in a QoS policy map.
set discard-class	Assigns a discard-class value for a class of traffic in a QoS policy map.
show class-map qos	Displays class maps.
show policy-map	Displays policy maps and statistics.

class-map

To create or modify a QoS class map that defines a class of traffic, use the **class-map** command. To remove a class map, use the **no** form of this command.

class-map [**type qos**] [**match-any** | **match-all**] *class-map-name*

no class-map [**type qos**] [**match-any** | **match-all**] *class-map-name*

Syntax Description

type qos	(Optional) Specifies the component type QoS for the class map. By default, the class map type is QoS.
match-any	(Optional) Specifies that if the packet matches any of the matching criteria configured for this class map, then this class map is applied to the packet.
match-all	(Optional) Specifies that if the packet matches all the matching criteria configured for this class map, then this class map is applied to the packet. This is the default action if **match-any** is not specified.
class-map-name	Name assigned to the class map. The name class-default is reserved.

Defaults

type QoS

match-all

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Hyphen, underscore, and alphabetic characters are allowed in the class map name.

Forty characters are the maximum allowed in the class map name.

Characters in the class map name are case sensitive.

Examples

This example shows how to create a class map and enter the QoS class map configuration mode to configure the specified map:

```
n1000v# configure terminal
n1000v(config)# class-map my_class1
n1000v(config-cmap-qos)#
```

This example shows how to remove the QoS class map named *my_class1*:

```
n1000v(config)# no class-map my_class1
```

```
n1000v(config)#
```

Related Commands

Command	Description
show class-map qos	Displays class maps.
match class-map	Configures the traffic class by matching packets based on match criteria in another class map.
match packet length	Configures the traffic class by matching packets based on packet lengths.

class-map type queuing

To modify a type queuing class map and enter the class-map configuration mode, use the **class-map type queuing** command.

class-map type queuing {match-any | match-all} *queuing-class-map-name*

Syntax Description

match-any	Specifies that if the packet matches any of the matching criteria configured for this class map, then this class map is applied to the packet.
match-all	Specifies that if the packet matches all the matching criteria configured for this class map, then this class map is applied to the packet. This is the default action if **match-any** is not specified.
queuing-class-map-name	Name assigned to the class map. The name class-default is reserved.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to modify a queuing class map:

```
n1000v(config)# class-map type queuing match-any myclass
n1000v(config-cmap-que)#
```

Related Commands

Command	Description
show class-map type queuing	Displays class maps.
match cos	Configures the traffic class by matching packets based on match criteria in another class map.
match protocol	Configures match criteria based on protocol.

clear access-list counters

To clear the counters for IP and MAC access control list(s) (ACLs), use the **clear access-list counters** command.

clear access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

If you specify an ACL, the name can be up to 64 alphanumeric, case-sensitive characters.

Examples

This example shows how to clear counters for all IP and MAC ACLs:

```
n1000v# clear access-list counters
n1000v#
```

This example shows how to clear counters for an IP ACL named acl-ip-01:

```
n1000v# clear access-list counters acl-ip-01
n1000v#
```

Related Commands

Command	Description
clear ip access-list counters	Clears counters for IP ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.
show access-lists	Displays information about one or all IP and MAC ACLs.

clear active-active accounting logs

To clear the accounting logs that are stored on a local VSM during the split-brain resolution, use the **clear active-active accounting logs** command.

clear active-active accounting logs

Syntax Description

This command has no arguments.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2.1SV2(1.1)	This command was introduced.

Usage Guidelines

Use the following command to check the accounting logs that were backed up during the split-brain resolution.

Examples

This example shows how to clear the accounting logs:

```
n1000v# clear active-active accounting logs
n1000v#
```

Related Commands

Command	Description
clear active-active remote accounting logs	Clears the remote accounting logs that are stored on a remote VSM during the split-brain resolution.
clear active-active redundancy traces	Clears the redundancy traces that are stored on a local VSM during the split-brain resolution.
clear active-active remote redundancy traces	Clears the remote redundancy traces that are stored on a remote VSM during the split-brain resolution.

clear active-active remote accounting logs

To clear the remote accounting logs that are stored on a remote VSM during the split-brain resolution, use the **clear active-active remote accounting logs** command.

clear active-active remote accounting logs

Syntax Description

This command has no arguments.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2.1SV2(1.1)	This command was introduced.

Usage Guidelines

Use the following command to check the remote accounting logs that were backed up during the split-brain resolution.

Examples

This example shows how to clear the remote accounting logs:

```
n1000v# clear active-active remote accounting logs
n1000v#
```

Related Commands

Command	Description
clear active-active accounting logs	Clears the accounting logs that are stored on a local VSM during the split-brain resolution.
clear active-active redundancy traces	Clears the redundancy traces that are stored on a local VSM during the split-brain resolution.
clear active-active remote redundancy traces	Clears the remote redundancy traces that are stored on a remote VSM during the split-brain resolution.

clear active-active redundancy traces

To clear the redundancy traces that are stored on a local VSM during the split-brain resolution, use the **clear active-active redundancy traces** command.

clear active-active redundancy traces

Syntax Description This command has no arguments.

Defaults None

Command Modes Any

SupportedUserRoles network-admin

Command History

Release	Modification
4.2.1SV2(1.1)	This command was introduced.

Usage Guidelines Use the following command to check the redundancy traces that were backed up during the split-brain resolution.

Examples This example shows how to clear the redundancy traces:

```
n1000v# clear active-active redundancy traces
n1000v#
```

Related Commands

Command	Description
clear active-active accounting logs	Clears the accounting logs that are stored on a local VSM during the split-brain resolution.
clear active-active remote accounting logs	Clears the remote accounting logs that are stored on a remote VSM during the split-brain resolution.
clear active-active remote redundancy traces	Clears the remote redundancy traces that are stored on a remote VSM during the split-brain resolution.

clear active-active remote redundancy traces

To clear the remote accounting logs that are stored on a remote VSM during the split-brain resolution, use the **clear active-active remote redundancy traces** command.

clear active-active remote redundancy traces

Syntax Description

This command has no arguments.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2.1SV2(1.1)	This command was introduced.

Usage Guidelines

Use the following commands to check the remote accounting logs that were backed up during the split-brain resolution.

Examples

This example shows how to clear the remote accounting logs:

```
n1000v# clear active-active remote redundancy traces
n1000v#
```

Related Commands

Command	Description
clear active-active accounting logs	Clears the accounting logs that are stored on a local VSM during the split-brain resolution.
clear active-active remote accounting logs	Clears the remote accounting logs that are stored on a remote VSM during the split-brain resolution.
clear active-active redundancy traces	Clears the redundancy traces that are stored on a local VSM during the split-brain resolution.

clear cdp

To clear Cisco Discovery Protocol (CDP) information on an interface, use the **clear cdp** command.

clear cdp {**counters** [**interface** *slot/port*] | **table** [**interface** *slot/port*]}

Syntax Description

counters	Clear CDP counters on all interfaces.
interface *slot/port*	(Optional) Clear CDP counters on a specified interface .
table	Clear CDP cache on all interfaces.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

network-operator

Command History

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

Examples

This example shows how to clear CDP counters on all interfaces:

```
n1000V# clear cdp counters
```

This example shows how to clear CDP cache on all interfaces:

```
n1000V# clear cdp table
```

Related Commands

Command	Description
show cdp all	Displays all interfaces that have CDP enabled.
show cdp entry	Displays the CDP database entries
show cdp global	Displays the CDP global parameters.
show cdp interface *intrface-type slot-port*	Displays the CDP interface status

clear cli history

To clear the history of commands you have entered into the CLI, use the **clear cli history** command.

clear cli history

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use the **show cli history** command to display the history of the commands that you entered at the command-line interface (CLI).

Examples

This example shows how to clear the command history:

```
n1000v# clear cli history
```

Related Commands

Command	Description
show cli history	Displays the command history.

clear cores

To clear the core files, use the **clear cores** command.

clear cores [**archive**]

Syntax Description		
	archive	(Optional) Clears the core file on the logflash filesystem.

Defaults None

Command Modes Any

SupportedUserRoles network-admin

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

Usage Guidelines Use the **show system cores** command to display information about the core files.

Examples This example shows how to clear the core file:

```
n1000v# clear cores
```

This example shows how to clear the core on the logflash filesystem:

```
n1000v# clear cores archive
```

Related Commands	Command	Description
	show system cores	Displays the core filename.
	system cores	Configures the core filename.

clear counters

To clear interface counters, use the **clear counters** command.

clear counters [interface {all | ethernet *slot/port* **| loopback** *virtual-interface-number* **| mgmt | port-channel** *port-channel-number* **| vethernet** *interface-number***}]**

Syntax Description

interface	Clears interface counters.
all	Clears all interface counters.
ethernet *slot/port*	Clears Ethernet interface counters. The range is 1 to 66.
loopback *virtual-interface-number*	Clears loopback interface counters. The range is 0 to 1023.
mgmt	Clears the management interface (mgmt0).
port-channel *port-channel-number*	Clears port-channel interfaces. The range is 1 to 4096.
vethernet *interface-number*	Clears virtual Ethernet interfaces. The range is 1 to 1048575.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

network-operator

Command History

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

Examples

This example shows how to clear the Ethernet interface counters:

```
n1000v(config)# clear counters ethernet 2/1
```

Related Commands

Command	Description
show interface counters	Displays the interface status, which includes the counters.

clear debug-logfile

To clear the contents of the debug logfile, use the **clear debug-logfile** command.

clear debug-logfile *filename*

Syntax Description

filename	Name of the debug logfile to clear.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to clear the debug logfile:

```
n1000v# clear debug-logfile syslogd_debugs
```

Related Commands

Command	Description
debug logfile	Configures a debug logging file.
debug logging	Enable debug logging.
show debug logfile	Displays the contents of the debug logfile.

clear flow exporter

To clear the statistics for a Flexible NetFlow flow exporter, use the **clear flow exporter** command in Any.

clear flow exporter {**name** *exporter-name* | *exporter-name*}

Syntax Description

name	Indicates that a flow exporter will be specified by name.
exporter-name	Name of an existing flow exporter.

Command Default

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

You must have already enabled traffic monitoring with Flexible NetFlow using an exporter before you can use the **clear flow exporter** command.

Examples

The following example clears the statistics for the flow exporter named NFC-DC-PHOENIX:

```
n1000v# clear flow exporter name NFC-DC-PHOENIX
n1000v#
```

Related Commands

Command	Description
clear flow exporter	Clears the statistics for exporters.
flow exporter	Creates a flow exporter.
show flow exporter	Displays flow exporter status and statistics.

clear ip access-list counters

To clear the counters for IP access control lists (ACLs), use the **clear ip access-list counters** command.

clear ip access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IP ACL whose counters you want cleared. The name can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

If specifying an ACL by name, it can be up to 64 alphanumeric, case-sensitive characters.

Examples

This example shows how to clear counters for all IP ACLs:

```
n1000v# clear ip access-list counters
n1000v#
```

This example shows how to clear counters for an IP ACL named acl-ip-101:

```
n1000v# clear ip access-list counters acl-ip-101
n1000v#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IP and MAC ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.
show access-lists	Displays information about one or all IP and MAC ACLs.
show ip access-lists	Displays information about one or all IP ACLs.

clear ipv6 access-list counters

To clear the counters for IPv6 access control lists (ACLs), use the **clear ipv6 access-list counters** command.

clear ipv6 access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 ACL whose counters you want cleared. The name can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Usage Guidelines

If specifying an ACL by name, it can be up to 64 alphanumeric, case-sensitive characters.

Examples

This example shows how to clear counters for all IPv6 ACLs:

```
n1000v# clear ipv6 access-list counters
n1000v#
```

This example shows how to clear counters for an IPv6 ACL named acl-ip-101:

```
n1000v# clear ipv6 access-list counters acl-ipv6-101
n1000v#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6 and MAC ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.
show access-lists	Displays information about one or all IPv4, IPv6 and MAC ACLs.
show ip access-lists	Displays information about one or all IPv4 ACLs.
show ipv6 access-lists	Displays information about one or all IPv6 ACLs.

clear ip arp inspection statistics vlan

To clear the Dynamic ARP Inspection (DAI) statistics for a specified VLAN, use the **clear ip arp inspection statistics vlan** command.

clear ip arp inspection statistics vlan *vlan-list*

Syntax Description

vlan-list	Range of VLAN IDs from 1 to 4094 that you can clear DAI statistics from.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to clear the DAI statistics for VLAN 2:

```
n1000v# clear ip arp inspection statistics vlan 2
n1000v#
```

This example shows how to clear the DAI statistics for VLANs 5 through 12:

```
n1000v# clear ip arp inspection statistics vlan 5-12
n1000v#
```

This example shows how to clear the DAI statistics for VLAN 2 and VLANs 5 through 12:

```
n1000v# clear ip arp inspection statistics vlan 2,5-12
n1000v#
```

Related Commands

Command	Description
ip arp inspection vlan	Enables or disables DAI for a list of VLANs.
show ip arp inspection statistics	Displays the DAI statistics.

clear ip dhcp snooping binding

To clear dynamically added entries from the DHCP snooping binding database, use the **clear ip dhcp snooping binding** command.

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*]

Syntax Description

vlan	(Optional) Specifies the VLAN to clear.
vlan-id	ID of the specified VLAN.
mac	(Optional) Specifies the MAC address associated with this VLAN.
mac-addr	MAC address associated with this VLAN.
ip	(Optional) Specifies the IP address associated with this VLAN.
ip-addr	IP address associated with this VLAN.
interface	(Optional) Specifies the interface associated with this VLAN.
interface-id	ID of the interface.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

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

Examples

This example shows how to clear dynamically added entries from the DHCP snooping binding database:

```
n1000v# clear ip dhcp snooping binding
n1000v#
```

This example shows how to clear a DHCP snooping binding table entry for an interface:

```
n1000v# clear ip dhcp snooping binding vlan 10 mac EEEE.EEEE.EEEE ip 10.10.10.1 interface
vethernet 1
n1000v#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
show ip dhcp snooping binding	Displays the DHCP snooping binding database.

Command	Description
ip dhcp snooping	Enables DHCP snooping globally.
ip dhcp snooping vlan	Enables DHCP snooping on the VLANs specified by *vlan-list*.
ip dhcp snooping verify mac-address	Enables DHCP snooping MAC address verification.

clear ip igmp interface statistics

To clear the IGMP statistics for an interface, use the **clear ip igmp interface statistics** command.

clear ip igmp interface statistics [*if-type if-number*]

Syntax Description

if-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
if-number	(Optional) Interface number.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

network-operator

Command History

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

Examples

This example shows how to clear IGMP statistics for an interface:

```
n1000v# clear ip igmp interface statistics ethernet 2/1
n1000v#
```

Related Commands

Command	Description
show ip igmp interface	Displays information about IGMP interfaces.

clear ip igmp snooping statistics vlan

To clear the IGMP snooping statistics for VLANs, use the **clear ip igmp snooping statistics vlan** command.

clear ip igmp snooping statistics vlan {*vlan-id* | **all**}

Syntax Description

vlan-id	VLAN number. The range is from 1 to 3967 and 4048 to 4093.
all	Applies to all VLANs.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

network-operator

Command History

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

Examples

This example shows how to clear IGMP snooping statistics for VLAN 1:

```
n1000v# clear ip igmp snooping statistics vlan 1
n1000v#
```

Related Commands

Command	Description
show ip igmp snooping statistics vlan	Displays IGMP snooping statistics by VLAN.

clear lacp counters

To clear the statistics for all interfaces for Link Aggregation Control Protocol (LACP) groups, use the **clear lacp counters** command.

clear lacp counters [**interface port-channel** *channel-number*]

Syntax Description

channel-number	(Optional) LACP port-channel number. The range of values is from 1 to 4096.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

If you clear counters for a specific port channel, the allowable port channel numbers are from 1 to 4096.

If you do not specify a channel number, the LACP counters for all LACP port groups are cleared.

If you clear counters for a static port-channel group, without the aggregation protocol enabled, the device ignores the command.

Examples

This example shows how to clear all the LACP counters:

```
n1000v(config)# clear lacp counters
n1000v(config) #
```

This example shows how to clear all LACP counters for the LACP port-channel group 20:

```
n1000v(config)# clear lacp counters interface port-channel 20
n1000v(config)#
```

Related Commands

Command	Description
show lacp counters	Displays information about LACP statistics.

clear license

To uninstall a license file from a VSM, or to uninstall an evaluation license before installing a permanent license, use the **clear license** command.

clear license *filename*

Syntax Description

filename	Name of the license file to be uninstalled.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

If a license is in use, you cannot uninstall it. Before uninstalling the license file, all licenses must first be transferred from the VEMs to the VSM license pool.

Caution **Service Disruption**
When you uninstall a license file from a VSM, the vEthernet interfaces on the VEMs are removed from service and the traffic flowing to them from virtual machines is dropped. This traffic flow is not resumed until you add a new license file with licenses for the VEMs. We recommend notifying the server administrator that you are uninstalling a license and that this will cause the vEthernet interfaces to shut down.

Examples

This example shows how to remove the Enterprise.lic license file from a VSM:

```
n1000v# clear license Enterprise.lic
Clearing license Enterprise.lic:
SERVER this_host ANY
VENDOR cisco

Do you want to continue? (y/n) y
Clearing license ..done
n1000v#
```

Related Commands

Command	Description
show license	Displays license information.
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.

clear line

To end a session on a specified vty, use the **clear line** command.

clear line *word*

Syntax Description		
	word	Specifies the vty name.

Defaults None

Command Modes Any

SupportedUserRoles network-admin
network-operator

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

Examples This example shows how to end a session on a specified vty:

```
n1000v(config)# clear line
```

Related Commands	Command	Description
	show users	Displays active user sessions.

clear logging logfile

Use the **clear logging logfile** command to clear messages from the logging file.

clear logging logfile

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

Super user

Command History

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

Examples

This example shows how to clear messages from the logging file:

```
n1000v# clear logging logfile
n1000v#
```

Related Commands

Command	Description
show logging logfile	Displays the logs in the local log file.

clear logging session

Use the **clear logging session** command to clear the current logging session.

clear logging session

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any

SupportedUserRoles Super user

Command History

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

Examples This example shows how to clear the current logging session:

```
n1000v# clear logging session
n1000v#
```

Related Commands

Command	Description
show logging session	Displays logging session status

clear mac access-list counters

To clear the counters for MAC access control lists (ACLs), use the **clear mac access-list counters** command.

clear mac access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the MAC ACL whose counters you want to clear. The name can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

If you want counters cleared for a specific MAC ACL, the name can be up to 64 alphanumeric, case-sensitive characters.

Examples

This example shows how to clear counters for all MAC ACLs:

```
n1000v# clear mac access-list counters
n1000v#
```

This example shows how to clear counters for a MAC ACL named acl-mac-0060:

```
n1000v# clear mac access-list counters acl-mac-0060
n1000v#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IP and MAC ACLs.
clear ip access-list counters	Clears counters for IP ACLs.
show access-lists	Displays information about one or all IP and MAC ACLs.
show mac access-lists	Displays information about one or all MAC ACLs.

clear mac address-table dynamic

To clear the dynamic address entries from the MAC address table in Layer 2, use the **clear mac address-table dynamic** command.

clear mac address-table dynamic [[**address** *mac-addr*] [**vlan** *vlan-id*] [**interface** {*type slot/port* | **port-channel** *number*}]

Syntax Description

address *mac-addr*	(Optional) Specifies the MAC address to remove from the table. Use the format XXXX.XXXX.XXXX.
vlan *vlan-id*	(Optional) Specifies the VLAN from which the MAC address should be removed from the table. The range of valid values is from 1 to 4094.
interface {*type slot/port* | **port-channel** *number*}]	(Optional) Specifies the interface. Use either the type of interface, the slot number, and the port number, or the port-channel number.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use the **clear mac address-table dynamic** command with no arguments to remove all dynamic entries from the table.

To clear static MAC addresses from the table, use the **no mac address-table static** command.

If the **clear mac address-table dynamic** command is entered with no options, all dynamic addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, the device removes all addresses on the specified interfaces.

Examples

This example shows how to clear all the dynamic Layer 2 entries from the MAC address table:

```
n1000v(config)# clear mac address-table dynamic
n1000v(config) #
```

This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:

```
n1000v(config)# clear mac address-table dynamic vlan 20 interface ethernet 2/20
n1000v(config)#
```

Related Commands

Command	Description
show mac address-table	Displays the information about the MAC address table.

clear mac address-table sw-installed stale-entries

To clear the software installed address entries from the MAC address table. Clear commands allow for clearing up any stale MACs/VTEPs.

clear mac address-table sw-installed stale entries

Syntax Description

sw-installed	Specifies that you want to clear software installed MAC addresses and VTEPs.
stale entries	Specifies any stale MACs/VTEPs entries.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

network-operator

Command History

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

Usage Guidelines

Use the **clear mac address-table sw-installed stale entries** command to clear the software installed MAC addresses and any stale entries in the VSM.

Examples

This example shows how to clear the software installed address entries from the MAC address table:

n1000v(config)# **clear mac address-table sw-installed stale-entries**

Related Commands

Command	Description
clear mac address-table sw-installed stale-entries module <module num>	To clear the software installed MAC addresses of specific module.
clear vtep-table stale-entries	To clear the stale VTEPs entries.
clear vtep-table stale-entries module <module num>	To clear the stale VTEPs entries of specific module.

clear mac address-table sw-installed stale-entries module <module num>

To clear the software installed address entries from the MAC address table of specific module. Clear commands allow for clearing up any stale MACs/VTEPs.

clear mac address-table sw-installed stale-entries module <module num>

Syntax Description

sw-installed	Specifies that you want to clear software installed MAC addresses and VTEPs.
stale entries	Specifies any stale MACs/VTEPs entries.
module <module num>	Specifies the specific module number.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

network-operator

Command History

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

Usage Guidelines

Use the **clear mac address-table sw-installed stale-entries module <module num>** command to clear the software installed MAC addresses and any stale entries of the specific module in the VSM.

Examples

This example shows how to clear the software installed address entries from the MAC address table of specific module:

n1000v(config)# **clear mac address-table sw-installed stale-entries module <module num>**

Related Commands

Command	Description
clear mac address-table sw-installed stale-entries	To clear the software installed MAC addresses.
clear vtep-table stale-entries	To clear the stale VTEPs entries.
clear vtep-table stale-entries module <module num>	To clear the stale VTEPs entries of specific module.

clear ntp statistics

To clear the Network Time Protocol statistics, use the **clear ntp statistics** command.

clear ntp statistics {**all-peers** | **io** | **local** | **memory**}

Syntax Description

all-peers	Clear statistics for all NTP peers.
io	Clear IO statistics.
local	Clear local statistics.
memory	Clear memory statistics.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

network-operator

Command History

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

Examples

This example shows how to clear statistics for all NTP peers:

```
n1000v(config)# clear ntp statistics all-peers
```

Related Commands

Command	Description
show ntp peers	Displays information about NTP peers.

clear port-security

To clear dynamically-learned, secure MAC address(es), use the **clear port-security** command.

clear port-security {**dynamic**} {**interface vethernet** *veth-number* | **address** *address* **module** *module-number*} [**vlan** *vlan-id*]

Syntax Description

dynamic	Specifies that you want to clear dynamically-learned, secure MAC addresses.
interface vethernet *veth-number*	Specifies the interface of the dynamically learned, secure MAC addresses that you want to clear.
address *address*	Specifies a single MAC address to be cleared, where *address* is the MAC address.
vlan *vlan-id*	Specifies the VLAN of the secure MAC addresses to be cleared. Valid VLAN IDs are from 1 to 4096.
module	Module number.

Defaults

dynamic

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to remove dynamically learned, secure MAC addresses from the veth1 interface:

```
n1000v# config t
n1000v(config)# clear port-security dynamic interface veth 1
```

This example shows how to remove the dynamically learned, secure MAC address 0019.D2D0.00AE:

```
n1000v# config t
n1000v(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Related Commands

Command	Description
debug port-security	Provides debugging information for port security.
switchport port-security	Enables port security on a Layer 2 interface.

clear qos statistics

To clear the counters for QoS statistics, use the **clear qos statistics** command.

clear qos statistics {**interface** [**ethernet** *type/slot* | **vethernet** *number* | **port-channel** *number*] } [**input type qos** | **output type qos**]}

Syntax Description

interface	(Optional) Identifies a specific interface for which to clear statistics.
input type qos	(Optional) Clears only input QoS statistics.
output type qos	(Optional) Clears only output QoS statistics.

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

If you do not specify an interface, the counters are cleared for all interfaces.

Examples

This example shows how to clear QoS statistics for all interfaces:

```
n1000v# clear qos statistics
n1000v#
```

This example shows how to clear all input QoS statistics for veth2:

```
n1000v# clear qos statistics veth2 input type qos
n1000v#
```

Related Commands

Command	Description
qos statistics	Enables or disables QoS statistics.
show policy-map	Displays the policy map configuration for all policy maps or for a specified policy map.

clear ssh hosts

To clear the Secure Shell (SSH) host sessions, use the **clear ssh hosts** command.

clear ssh hosts

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to clear all SSH host sessions:

```
n1000v# clear ssh hosts
```

Related Commands

Command	Description
ssh server enable	Enables the SSH server.

clear system reset-reason

To clear the device reset-reason history, use the **clear system reset-reason** command.

clear system reset-reason

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to clear reset-reason history:

```
n1000v# clear system reset-reason
```

Related Commands

Command	Description
show system reset-reason	Displays the device reset-reason history.

clear user

To clear a user session, use the **clear user** command.

clear user *user-id*

Syntax Description		
	user-id	User identifier.

Defaults None

Command Modes Any

SupportedUserRoles network-admin

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

Usage Guidelines Use the **show users** command to display the current user sessions on the device.

Examples This example shows how to clear all SSH host sessions:

```
n1000v# clear user user1
```

Related Commands	Command	Description
	show users	Displays the user session information.

clear vtep-table stale-entries

To clear the stale vteps entries from the address table. Clear commands allow for clearing up any stale MACs/VTEPs.

clear vtep-table stale-entries

Syntax Description

vtep-table	Specifies that you want to clear stale VTEPs.
stale-entries	Specifies any stale MACs/VTEPs entries.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use the **clear vtep-table stale-entries** command to clear the stale vtep entries in the VSM.

Examples

This example shows how to clear the stale vtep entries:

```
n1000v(config)# clear vtep-table stale-entries
```

Related Commands

Command	Description
clear mac address-table sw-installed stale-entries module <module num>	To clear the software installed MAC addresses of specific module.
clear mac address-table sw-installed stale-entries	To clear the software installed MAC addresses.
clear vtep-table stale-entries module <module num>	To clear the stale VTEPs entries of specific module.

clear vtep-table stale-entries module <module num>

To clear the stale vteps entries from the address table of specific module. Clear commands allow for clearing up any stale MACs/VTEPs.

clear vtep-table stale-entries module <module num>

Syntax Description

vtep-table	Specifies that you want to clear stale VTEPs.
stale-entries	Specifies any stale MACs/VTEPs entries.
module <module num>	Specifies the specific module number.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use the **clear vtep-table stale-entries module <module num>** command to clear the stale vtep entries of specific module.

Examples

This example shows how to clear the stale vtep entries of specific module:

```
n1000v(config)# clear vtep-table stale-entries module <module num>
```

Related Commands

Command	Description
clear mac address-table sw-installed stale-entries module <module num>	To clear the software installed MAC addresses of specific module.
clear mac address-table sw-installed stale-entries	To clear the software installed MAC addresses.
clear vtep-table stale-entries	To clear the stale VTEPs entries.

cli var name

To define a command line interface (CLI) variable for a terminal session, use the **cli var name** command. To remove the CLI variable, use the **no** form of this command.

cli var name *variable-name variable-text*

cli no var name *variable-name*

Syntax Description

variable-name	Name of the variable. The name is alphanumeric, case sensitive, and has a maximum of 31 characters.
variable-text	Variable text. The text is alphanumeric, can contain spaces, and has a maximum of 200 characters.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

You can reference a CLI variable using the following syntax:

$(variable-name**)**

Instances where you can use variables in include the following:

- Command scripts
- Filenames

You cannot reference a variable in the definition of another variable.

You can use the predefined variable, TIMESTAMP, to insert the time of day. You cannot change or remove the TIMESTAMP CLI variable.

You must remove a CLI variable before you can change its definition.

Examples

This example shows how to define a CLI variable:

```
n1000v# cli var name testinterface interface 2/3
```

This example shows how to reference the TIMESTAMP variable:

```
n1000v# copy running-config > bootflash:run-config-$(TIMESTAMP).cnfg
```

This example shows how to remove a CLI variable:

```
n1000v# cli no var name testinterface interface 2/3
```

Related Commands

Command	Description
show cli variables	Displays the CLI variables.

clock set

To manually set the clock, use the **clock set** command.

clock set *time day month year*

Syntax Description

time	Time of day. The format is *HH*:*MM*:*SS*.
day	Day of the month. The range is from 1 to 31.
month	Month of the year. The values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**.
year	Year. The range is from 2000 to 2030.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use this command when you cannot synchronize your device with an outside clock source, such as NTP.

Examples

This example shows how to manually set the clock:

```
n1000v# clock set 9:00:00 1 June 2008
```

Related Commands

Command	Description
show clock	Displays the clock time.

clock summer-time

To configure the summer-time (daylight saving time) offset, use the **clock summer-time** command. To revert to the default, use the **no** form of this command.

clock summer-time *zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes*

no clock summer-time

Syntax Description

zone-name	Time zone string. The time zone string is a three-character string.
start-week	Week of the month to start the summer-time offset. The range is from 1 to 5.
start-day	Day of the month to start the summer-time offset. Valid values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
start-month	Month to start the summer-time offset. Valid values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**.
start-time	Time to start the summer-time offset. The format is *hh*:*mm*.
end-week	Week of the month to end the summer-time offset. The range is from 1 to 5.
end-day	Day of the month to end the summer-time offset. Valid values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
end-month	Month to end the summer-time offset. Valid values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**.
end-time	Time to end the summer-time offset. The format is *hh*:*mm*.
offset-minutes	Number of minutes to offset the clock. The range is from 1 to 1440.

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 configure the offset for summer-time or daylight saving time:

```
n1000v# configure terminal
n1000v(config)# clock summer-time PDT 1 Sunday March 02:00 1 Sunday November 02:00 60
```

This example shows how to remove the summer-time offset:

```
n1000v# configure terminal
n1000v(config)# no clock summer-time
```

Related Commands

Command	Description
show clock	Displays clock summer-time offset configuration.

clock timezone

To configure the time zone offset from Coordinated Universal Time (UTC), use the **clock timezone** command. To revert to the default, use the **no** form of this command.

clock timezone *zone-name offset-hours offset-minutes*

no clock timezone

Syntax Description

zone-name	Zone name. The name is a 3-character string for the time zone acronym (for example, PST or EST).
offset-hours	Number of hours offset from UTC. The range is from –23 to 23.
offset-minutes	Number of minutes offset from UTC. The range is from 0 to 59.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to configure the time zone offset from UTC:

```
n1000v# clock timezone EST 5 0
```

This example shows how to remove the time zone offset:

```
n1000v# no clock timezone
```

Related Commands

Command	Description
show clock	Displays the clock time.

cluster-id A.B.C.D

To configure Route Reflector Cluster-ID, use the **cluster-id A.B.C.D** command.

cluster-id A.B.C.D

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any

SupportedUserRoles network-admin
network-operator

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples This example shows how to manually specify the IP address to use as cluster-id for Route Reflector:

```
n1000v(config-router)# cluster-id 17.17.17.31
```

Related Commands

Command	Description
show clock	Displays the clock time.

collect counter

To configure the number of bytes or packets in a flow as a non-key field and collect the number of bytes or packets seen for a Flexible NetFlow flow record, use the **collect counter** command. To disable the counters, use the **no** form of this command.

collect counter {**bytes** [**long**] | **packets** [**long**]}

no collect counter {**bytes** [**long**] | **packets** [**long**]}

Syntax Description

bytes	Configures the number of bytes or packets seen in a flow as a non-key field and enables collecting the total number of bytes from the flow.
long	(Optional) Enables collecting the total number of bytes from the flow using a 64 bit counter.
packets	Configures the number of bytes seen in a flow as a non-key field and enables collecting the total number of packets from the flow.

Command Default

This command is not enabled by default.

Command Modes

Flow record configuration (config-flow-record)

SupportedUserRoles

network-admin

Command History

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

Examples

The following example enables collecting the total number of bytes from the flows as a non-key field:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter bytes
```

The following example enables collecting the total number of bytes from the flows as a non-key field using a 64 bit counter:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter bytes long
```

The following example enables collecting the total number of packets from the flows as a non-key field:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter packets
```

The following example enables collecting the total number of packets from the flows as a non-key field using a 64 bit counter:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter packets long
```

Related Commands

Command	Description
collect counter	Configures the counters as a non-key field and collects the counter values.
flow record	Creates a flow record.
show flow record	Displays flow record status and statistics.

collect timestamp sys-uptime

To collect the TIMESTAMP SYS-UPTIME for a NetFlow flow record, use the **collect timestamp sys-uptime** command. To disable the collection, use the **no** form of this command.

collect timestamp sys-uptime {**first** | **last**}

no collect timestamp sys-uptime {**first** | **last**}

Syntax Description

first	Configures the sys-uptime for the time the first packet was seen from the flows as a non-key field and enables collecting time stamps based on the sys-uptime for the time the first packet was seen from the flows.
last	Configures the sys-uptime for the time the last packet was seen from the flows as a non-key field and enables collecting time stamps based on the sys-uptime for the time the most recent packet was seen from the flows.

Command Default

This command is not enabled by default.

Command Modes

Flow record configuration (config-flow-record)

SupportedUserRoles

network-admin

Command History

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

Examples

The following example enables collecting the sys-uptime for the time the first packet was seen from the flows:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect timestamp sys-uptime first
```

The following example enables collecting the sys-uptime for the time the most recent packet was seen from the flows:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect timestamp sys-uptime last
```

Related Commands

Command	Description
flow record	Creates a flow record.
show flow record	Displays flow record status and statistics.

collect transport tcp flags

To collect a Transmission Control Protocol (TCP) flags for a NetFlow flow record, use the **collect transport tcp flags** command. To disable the collection, use the **no** form of this command.

collect transport tcp flags

no collect transport tcp flags

Syntax Description

This command has no arguments or keywords

Command Default

This command is not enabled by default.

Command Modes

Flow record configuration (config-flow-record)

SupportedUserRoles

network-admin

Command History

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

Examples

The following example collects the TCP flags:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect transport tcp flags
```

Related Commands

Command	Description
flow record	Creates a flow record.
show flow record	Displays flow record status and statistics.

configure terminal

To access configuration commands in the CLI global configuration mode, use the **configure terminal** command.

configure terminal

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The configuration changes you make in the global configuration mode are saved in the running configuration file. To save these changes persistently across reboots and restarts, you must copy them to the startup configuration file using the **copy running-config startup-config** command.

Examples

This example shows how to access configuration commands in the CLI global configuration mode:

```
n1000v# configure terminal
n1000v(config)#
```

Related Commands

Command	Description
where	Displays the current configuration mode context.
pwd	Displays the name of the present working directory.
copy run start	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

connect

To initiate a connection with vCenter, use the **connect** command. To disconnect from vCenter, use the **no** form of this command.

connect

no connect

Syntax Description

This command has no arguments or keywords.

Defaults

no connect

Command Modes

SVS connect configuration (config-svs-conn)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Upon connection to vCenter, if a username and password have not been configured for this connection, you are prompted to enter them.

There can be only one active connection at a time. If a previously-defined connection is up, an error message displays and the **connect** command is rejected until the previous connection is closed by entering **no connect**.

Examples

This example shows how to connect to vCenter:

```
n1000v(config#) svs connection vcWest
n1000v(config-svs-conn#) protocol vmware-vim
n1000v(config-svs-conn#) remote hostname vcMain
n1000v(config-svs-conn#) vmware dvs datacenter-name HamiltonDC
n1000v(config-svs-conn#) connect
```

This example shows how to disconnect from vCenter:

```
n1000v(config#) svs connection vcWest
n1000v(config-svs-conn#) no connect
```

Related Commands

Command	Description
show svs connections	Displays the current connections to the Cisco Nexus 1000V.

control type multicast

Configures the control type multicast in Layer 3 mode on the VSM. To disable the control type multicast, use the no form of this command.

control type multicast

no control type multicast

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled by default.

Command Modes

SVS domain configuration (config-svs-domain)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

None.

Examples

The following example configures control type multicast::

```
n1000v(config)# svs-domain
n1000v(config-svs-domain)# control type multicast
```

Related Commands

Command	Description
show svs-domain	Displays svs domain configuration.

control vlan

To assign a control VLAN to the Cisco Nexus 1000V domain, use the **control vlan** command. To remove the control VLAN, use the **no** form of this command.

control vlan *number*

no control vlan

Syntax Description

number	control VLAN number.

Defaults

None

Command Modes

SVS domain configuration (config-svs-domain)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Newly-created VLANs remain unused until Layer 2 ports are assigned to them.

If you enter a VLAN ID that is assigned to an internally allocated VLAN, the CLI returns an error message.

Examples

This example shows how to configure control VLAN 70 for domain ID 32:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# domain id 32
n1000v(config-svs-domain)# control vlan 70
n1000v(config-svs-domain)#
```

This example shows how to remove control VLAN 70 from domain ID 32:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# domain id 32
n1000v(config-svs-domain)# no control vlan 70
n1000v(config-svs-domain)#
```

Related Commands

Command	Description
show vlan-id	Displays the configuration for the specified VLAN.
svs-domain	Creates the domain and places you into CLI SVS domain configuration mode.
domain id	Assigns a domain ID to the domain.
packet vlan	Assigns a packet VLAN to the domain.
show svs-domain	Displays the domain configuration.

copy

To copy a file from a source to a destination, use the **copy** command.

copy *source-url destination-url*

Syntax Description

source-url	Location URL (or variable) of the source file or directory to be copied. The source can be either local or remote, depending upon whether the file is being downloaded or uploaded.
destination-url	Destination URL (or variable) of the copied file or directory. The destination can be either local or remote, depending upon whether the file is being downloaded or uploaded.

The format of the source and destination URLs varies according to the file or directory location. You may enter either a command-line interface (CLI) variable for a directory or a filename that follows the Cisco NX-OS file system syntax (*filesystem*:[*/directory*][*/filename*]).

The following tables list URL prefix keywords by the file system type. If you do not specify a URL prefix keyword, the device looks for the file in the current directory.

Table 3-1 lists URL prefix keywords for bootflash and remote writable storage file systems.

Table 3-1 URL Prefix Keywords for Storage File Systems

Keyword	Source or Destination
bootflash:[*//module/*]	Source or destination URL for boot flash memory. The *module* argument value is **sup-active**, **sup-local**, **sup-remote**, or **sup-standby**.
ftp:	Source or destination URL for a FTP network server. The syntax for this alias is as follows: **ftp:**[*//server*][*/path*]*/filename*
scp:	Source or destination URL for a network server that supports Secure Shell (SSH) and accepts copies of files using the secure copy protocol (scp). The syntax for this alias is as follows: **scp:**[*//*[*username@*]*server*][*/path*]*/filename*
sftp:	Source or destination URL for an SSH FTP (SFTP) network server. The syntax for this alias is as follows: **sftp:**[*//*[*username@*]*server*][*/path*]*/filename*
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is as follows: **tftp:**[*//server*[**:***port*]][*/path*]*/filename*

Table 3-2 lists the URL prefix keywords for nonwritable file systems.

Table 3-2 URL Prefix Keywords for Special File Systems

Keyword	Source or Destination
core:	Local memory for core files. You can copy core files from the core: file system.
debug:	Local memory for debug files. You can copy core files from the debug: file system.
log:	Local memory for log files. You can copy log files from the log: file system.
system:	Local system memory. You can copy the running configuration to or from the system: file system. The system: file system is optional when referencing the running-config file in a command.
volatile:	Local volatile memory. You can copy files to or from the volatile: file system. All files in the volatile: memory are lost when the physical device reloads.

Defaults

The default name for the destination file is the source filename.

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The entire copying process may take several minutes, depending on the network conditions and the size of the file, and differs from protocol to protocol and from network to network.

The colon character (**:**) is required after the file system URL prefix keywords (such as **bootflash**).

In the URL syntax for **ftp:**, **scp:**, **sftp:**, and **tftp:**, the server is either an IP address or a host name.

Examples

This example shows how to copy a file within the same directory:

```
n1000v# copy file1 file2
```

This example shows how to copy a file to another directory:

```
n1000v# copy file1 my_files:file2
```

This example shows how to copy a file to another supervisor module:

```
n1000v# copy file1 bootflash://sup-remote/file1.bak
```

This example shows how to copy a file from a remote server:

```
n1000v# copy scp://10.10.1.1/image-file.bin bootflash:image-file.bin
```

Related Commands

Command	Description
cd	Changes the current working directory.
cli var name	Configures CLI variables for the session.
dir	Displays the directory contents.
move	Moves a file.
pwd	Displays the name of the current working directory.

copy running-config startup-config

To copy the running configuration to the startup configuration, use the **copy running-config startup-config** command.

copy running-config startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use this command to save configuration changes in the running configuration to the startup configuration in persistent memory. When a device reload or switchover occurs, the saved configuration is applied.

Examples

This example shows how to save the running configuration to the startup configuration:

```
n1000v# copy running-config startup-config
[########################################] 100%
```

Related Commands

Command	Description
show running-config	Displays the running configuration.
show running-config diff	Displays the differences between the running configuration and the startup configuration.
show startup-config	Displays the startup configuration.
write erase	Erases the startup configuration in the persistent memory.

cts device-id

To configure a Cisco TrustSec device identifier, use the **cts device-id** command.

cts device-id *device-id* **password [7]** *password*

Syntax Description

device-id	Cisco TrustSec device identifier name. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.
7	(Optional) Encrypts the password.
password *password*	Specifies the password to use during EAP-FAST processing. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Defaults

No Cisco TrustSec device identifier

Clear text password

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the feature cts command. The Cisco TrustSec device identifier name must be unique in your Cisco TrustSec network cloud. This command requires the Advanced Services license.

Examples

This example shows how to configure a Cisco TrustSec device identifier:

```
switch# configure terminal
swtich(config)# cts device-id DeviceA password Cisco321
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts credentials	Displays the Cisco TrustSec credentials information.

cts device tracking

To enable the device tracking on Cisco TrustSec SXP for Cisco Nexus 1000V, use the **cts device tracking** command. To disable the device tracking on Cisco TrustSec SXP, use the **no** form of this command.

cts device tracking

no cts device tracking

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)SV2(1.1)	This command was introduced.

Usage Guidelines

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to enable the device tracking on Cisco TrustSec SXP:

```
n1000v# configure terminal
n1000v(config)# cts device tracking
enabled
n1000v(config)#
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.
show cts device tracking	Displays the Cisco TrustSec device tracking configuration.

cts interface delete-hold

To configure the delete hold timer period for an interface, use the **cts interface delete-hold** command. To revert to the default, use the **no** form of this command.

cts interface delete-hold *seconds*

no cts interface delete-hold *seconds*

Syntax Description

seconds	Number of seconds. The range is from 0 to 64000.

Defaults

60 seconds.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

If the timer is set to 0, the IP-SGT mappings are deleted instantly.

The no form of this command does not start the timer when the interface goes to non-participating state and the IP-SGT entries are then always held on the interface.

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to configure the delete hold timer period for an interface:

```
n1000v# configure terminal
n1000v(config)# cts interface delete-hold
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.
show cts interface delete-hold timer	Displays the interface delete hold timer period for Cisco TrustSec

cts refresh role-based-policy

To refresh the Cisco TrustSec security group access control list (SGACL) policies downloaded from the Cisco Secure ACS, use the **cts refresh role-based-policy** command.

cts refresh role-based-policy

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode.

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. This command requires the Advanced Services license.

Examples

This example shows how to enter Cisco TrustSec manual configuration mode for an interface:

```
switch# cts refresh role-based-policy
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays Cisco TrustSec SGACL policy configuration.

cts role-based access-list

To create or specify a Cisco TrustSec security group access control list (SGACL) and enter role-based access control list configuration mode, use the **cts role-based access-list** command. To remove an SGACL, use the **no** form of this command.

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

Syntax Description

list-name	Name for the SGACL. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Defaults

None

Command Modes

Global configuration mode.

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. This command requires the Advanced Services license.

Examples

This example shows how to create a Cisco TrustSec SGACL and enter role-based access list configuration mode:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

This example shows how to remove a Cisco TrustSec SGACL:

```
switch# configure terminal
switch(config)# no cts role-based access-list MySGACL
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays Cisco TrustSec SGACL policy configuration.

cts role-based counters enable

To enable role-based access control list (RBACL) statistics, use the **cts role-based counters enable** command. To disabled RBACL statistics, use the no form of this command.

cts role-based counters enable

no cts role-based counters enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration mode.

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

To use this command, you must enable RBACL policy enforcement under the cts manual config mode at port-profiles conf.

When you enable RBACL statistics, each policy requires one entry in the . If you do not have enough space remaining in the , an error message appears, and you cannot enable the statistics.

When you modify an RBACL policy, statistics for the previously assigned access control entry (ACE) are displayed, and the newly assigned ACE statistics are initialized to 0.

RBACL statistics are lost only when the Cisco NX-OS device reloads or you deliberately clear the statistics.

Examples

This example shows how to enable RBACL statistics:

```
switch# configure terminal
switch(config)# cts role-based counters enable
```

This example shows how to disable RBACL statistics:

```
switch# configure terminal
switch(config)# no cts role-based counters enable
```

Related Commands

Command	Description
clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.
show cts role-based counters	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies.

cts role-based enforcement

To enable Cisco TrustSec security group access control list (SGACL) enforcement. use the **cts role-based enforcement** command under cys manual config level at port-profile configuration. To revert to the default, use the **no** form of this command.

cts role-based enforcement

no cts role-based enforcement

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

cts manual (at port-profile configuration)

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the feature cts command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Cisco TrustSec SGACL enforcement in a port-profile:

```
switch(config)# port-profile type vethernet A-PP
switch(config-port-prof)# cts manual
switch(config-port-prof-cts-manual)# role-based enforcement
switch(config-port-prof-cts-manual)# no role-based enforcement
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

cts role-based sgt

To manually configure mapping of Cisco TrustSec security group tags (SGTs) to a security group access control list (SGACL), use the **cts role-based sgt** command. To remove the SGT mapping to an SGACL, use the **no** form of this command.

cts role-based sgt { *sgt-value* **| any | unknown } dgt {** *dgt-value* **| unknown }**

access-list *list-name*

no cts role-based sgt { *sgt-value* **| any | unknown } dgt {** *dgt-value* **| unknown }**

Syntax Description

sgt-value	Source SGT value. The range is 0 to 65533.
any	Specifies any SGT.
unknown	Specifies an unknown SGT.
dgt	Specifies the destination SGT.
dgt-value	Destination SGT value. The range is 0 to 65533.
access-list *list-name*	Specifies the name for the SGACL.

Defaults

None.

Command Modes

Global configuration

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the feature cts command.

You must configure the SGACL before you can configure SGT mapping.

This command requires the Advanced Services license.

Examples

This example shows how to configure SGT mapping for an SGACL:

```
switch# configure terminal
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
```

This example shows how to remove SGT mapping for an SGACL:

```
switch# configure terminal
switch(config)# no cts role-based sgt 3 sgt 10
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays the Cisco TrustSec SGT mapping for an SGACL.

cts role-based sgt map

To manually configure the Cisco TrustSec security group tag (SGT) mapping to the host IP addresses, use the **cts role-based sgt-map** command. To remove an SGT, use the **no** form of this command.

cts role-based sgt-map *ip-address sgt*

no cts role-based sgt-map *ip-address sgt*

Syntax Description

ip-address	Specifies the IP address of the host.
sgt	Specifies the SGT corresponding to the IP address. The range is from 1-65519.

Defaults

None

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

You can use only IPv4 addressing with Cisco TrustSec.

The static IP-SGT bindings are configured in a context of a VRF and will be applied to the default VRF unless management VRF is specified.

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to configure mapping for a Cisco TrustSec SGT:

```
n1000v# configure terminal
n1000v(config)# cts role-based sgt-map 1.1.1.1 100
n1000v(config)#
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.
show cts role-based sgt-map	Displays the mapping of the IP address to SGT for Cisco TrustSec.
show ipstg entries	Displays SXP SGT mappings for Cisco TrustSec.

cts sgt

To configure the security group tag (SGT) for Cisco TrustSec, use the **cts sgt tag** command. To remove the SGT tag, use the **no** form of this command.

cts sgt *tag*

no cts sgt *tag*

Syntax Description

tag	Local SGT for the device that is a hexadecimal value with the format 0xhhhh. The range is from 1-65519.

Defaults

None

Command Modes

Port profile configuration (config-port-profile)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to configure the Cisco TrustSec SGT for the device:

```
n1000v# configure terminal
n1000v(config)# cts stg 0x00a2
n1000v(config)#
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.

cts sxp connection peer

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) peer connection for Cisco TrustSec, use the **cts sxp connection peer** command. To remove the SXP connection, use the **no** form of this command.

cts sxp connection peer *peer ip-address* **[source** *source ip-address* **] password {[default] | [none] | [required]** *password* **[mode { listener}] [vrf {default | management}**

no cts sxp connection peer *peer ip-address* **[source** *source ip-address* **] password {[default] | [none] | [required]** *password* **[mode { listener}] [vrf {default | management}**

Syntax Description

peer ip-address	Specifies IPv4 address of the peer device.
source ip-address	Specifies the IPV4 address of the source.
password	Specifies the password that SXP should use for the peer connection.
default	Specifies that SXP should use the default SXP password for the peer connection.
none	Specifies that SXP should not use a password for the peer connection.
required	Specifies the password that SXP should use for this peer connection.
mode	Specifies the mode of the peer device.
listener	Specifies that the peer is the listener.
vrf	Specifies the VRF for the peer.
default	Specifies the default VRF for the peer.
management	Specifies the management VRF for the peer.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

Since Cisco Nexus 1000V can only act as the speaker in the connection, the peer must be configured as the listener.

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to configure an SXP peer connection:

```
n1000v# configure terminal
n1000v(config)# cts sxp connection peer 1.2.3.4 password none mode listener vrf management
n1000v(config)#
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.
show cts sxp connection	Displays SXP connections for Cisco TrustSec.

cts sxp default password

To configure the default SXP password for the device, use the **cts sxp default password** command. To remove the default, use the **no** form of this command.

cts sxp default password[Word | 7] *password*

no cts sxp default password[Word | 7] *password*

Syntax Description

Word	Specifies unencrypted default password
7 password	Specifies encrypted default password.

Defaults

Unencrypted password.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to configure the default SXP password for the device:

```
n1000v# configure terminal
n1000v(config)# cts sxp default password 7 CisocPassword
n1000v(config)#
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.

cts sxp default source-ip

To configure the default SXP source IPv4 address for the device, use the **cts sxp default source-ip** command. To revert to the default, use the **no** form of this command.

cts sxp default source-ip *src-ip-addr*

no cts sxp default source-ip *src-ip-addr*

Syntax Description

src-ip-addr	Default SXP IPv4 address for the device.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

You can use only IPv4 addressing with Cisco TrustSec.

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to configure the default SXP source IP address for the device:

```
n1000v# configure terminal
n1000v(config)# cts sxp default source-ip 10.10.3.3
n1000v(config)#
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.
show cts sxp	Displays the SXP configuration for Cisco TrustSec.

cts sxp retry-period

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) retry period timer, use the **cts sxp retry-period** command. To revert to the default, use the **no** form of this command.

cts sxp retry-period *seconds*

no cts sxp retry-period *seconds*

Syntax Description

seconds	Number of seconds. The range is from 0 to 64000.

Defaults

60 seconds.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to configure the SXP retry period:

```
n1000v# configure terminal
n1000v(config)# cts sxp retry-period 120
n1000v(config)#
```

Related Commands

Command	Description
show cts	Displays Cisco TrustSec configuration.
show cts sxp	Displays the SXP configuration for Cisco TrustSec.

cts sxp enable

To enable the Security Group Tag (SGT) Exchange Protocol (SXP) peer on a device, use the **cts sxp enable command**. To revert to the default, use the **no** form of this command.

cts sxp enable

no cts sxp enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV2(1.1)	This command was introduced.

Usage Guidelines

This command requires an Advanced License. See the*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(1.1)* for more information on the licensing requirements for Cisco Nexus 1000V.

Examples

This example shows how to enable the Cisco TrustSec SXP:

```
n1000v# configure terminal
n1000v(config)# cts sxp enable
```

This example shows how to disable the Cisco TrustSec SXP:

```
n1000v# configure terminal
n1000v(config)# no cts sxp
```