S Commands

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

send

To send a message to an open session, use the **send** command.

send {*message* | **session** *device message*}

Syntax Description

message	Message.
session	Specifies a specific session.
device	Device type.

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 send a message to an open session:

```
n1000v# send session sessionOne testing
n1000v#
```

Related Commands

Command	Description
show banner	Displays a banner.

session-limit

To limit the number of VSH sessions, use the **session-limit** command. To remove the limit, use the **no** form of this command.

session-limit *number*

no session-limit *number*

Syntax Description

number	Number of VSH sessions. The range of valid values is 1 to 64

Defaults

No limit is set.

Command Modes

Line configuration (config-line)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to limit the number of VSH sessions:

```
n1000v# configure terminal
n1000v(config)# line vty
n1000v(config-line)# session-limit 10
n1000v(config-line)#
```

This example shows how to remove the limit:

```
n1000v# configure terminal
n1000v(config)# line vty
n1000v(config-line)# no session-limit 10
n1000v(config-line)#
```

service-policy

To configure a service policy for an interface, use the **service-policy** command. To remove the service policy configuration, use the **no** form of this command.

service-policy {**input** *name* [**no-stats**] | **output** *name* [**no-stats**] | **type qos** {**input** *name* [**no-stats**] | **output** *name* [**no-stats**]}}

no service-policy {**input** *name* [**no-stats**] | **output** *name* [**no-stats**] | **type qos** {**input** *name* [**no-stats**] | **output** *name* [**no-stats**]}}

Syntax Description

input	Specifies an input service policy.
name	Policy name. The range of valid values is 1 to 40.
no-stats	(Optional) Specifies no statistics.
output	Specifies an output service policy.
type qos	Specifies a QoS service policy.

Defaults

No service policy exists.

Command Modes

Interface Configuration (config-if)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to configure a service policy for an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 10
n1000v(config-if)# service-policy type qos input sp10 no-stats
n1000v(config-if)#
```

This example shows how to remove a service policy configuration for an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 10
n1000v(config-if)# no service-policy type qos input sp10 no-stats
n1000v(config-if)#
```

Related Commands

Command	Description
show running interface	Displays interface configuration information.

set

To set QoS class attributes, use the **set** command. To remove class attributes, use the **no** form of this command.

set {{**cos** *cos-val*} | {**dscp** [**tunnel**] {*dscp-val* | *dscp-enum*}} | {**precedence** [**tunnel**] {*prec-val* | *prec-enum*}} | {**discard-class** *dis-class-val*} | {**qos-group** *qos-grp-val*} | {{{**cos cos**} | {**dscp dscp**} | {**precedence precedence**} | {**discard-class discard-class**}} **table** *table-map-name*} | {**cos1** {{**dscp table cos-dscp-map**} | {**precedence table cos-precedence-map**} | {**discard-class table cos-discard-class-map**}}} | {**dscp1** {{**cos table dscp-cos-map**} | {**prec3 table dscp-precedence-map**} | {**dis-class3 table dscp-discard-class-map**}}} | {**prec1** {{**cos3 table precedence-cos-map**} | {**dscp3 table precedence-dscp-map**} | {**dis-class3 table precedence-discard-class-map**}}} | {**dis-class1** {{**cos3 table discard-class-cos-map**} | {**dscp3 table discard-class-dscp-map**} | {**prec3 table discard-class-precedence-map**}}}}

no set {{**cos** *cos-val*} | {**dscp** [**tunnel**] {*dscp-val* | *dscp-enum*}} | {**precedence** [**tunnel**] {*prec-val* | *prec-enum*}} | {**discard-class** *dis-class-val*} | {**qos-group** *qos-grp-val*} | {{{**cos cos**} | {**dscp dscp**} | {**precedence precedence**} | {**discard-class discard-class**}} **table** *table-map-name*} | {**cos1** {{**dscp table cos-dscp-map**} | {**precedence table cos-precedence-map**} | {**discard-class table cos-discard-class-map**}}} | {**dscp1** {{**cos table dscp-cos-map**} | {**prec3 table dscp-precedence-map**} | {**dis-class3 table dscp-discard-class-map**}}} | {**prec1** {{**cos3 table precedence-cos-map**} | {**dscp3 table precedence-dscp-map**} | {**dis-class3 table precedence-discard-class-map**}}} | {**dis-class1** {{**cos3 table discard-class-cos-map**} | {**dscp3 table discard-class-dscp-map**} | {**prec3 table discard-class-precedence-map**}}}}

Syntax Description

cos	Specifies IEEE 802.1Q CoS (Class of Service).
cos-value	CoS value. The range of valid values is 0 to 7.
dscp	Specifies DSCP (Differentiated Services Code Point) in IPv4 and IPv6 packets.
tunnel	(Optional) Specifies DSCP in tunnel encapsulation.
dscp-value	DSCP value.
dscp-enum	
precedence	Precedence in IP(v4) and IPv6 packets.
prec-val	IP Precedence value.
prec-enum	.
discard-class *dis-class-val*	Discard class + Discard class value.
qos-group *qos-grp-val*	Qos-group + Qos-group value.
table *table-map-name*	Table defining mapping from input to output + Table-map name.
cos1	IEEE 802.1Q class of service.
cos-dscp-map	Cos to DSCP Mutation map.
cos-precedence-map	Cos to Precedence Mutation map.
cos-discard-class-map	Cos to Discard Class Mutation map.

dscp1	DSCP in IP(v4) and IPv6 packets.
dscp-cos-map	DSCP to COS Mutation map.
prec3	Precedence in IP(v4) and IPv6 packets.
dscp-precedence-map	DSCP to Precedence Mutation map.
dis-class3	Discard class.
dscp-discard-class-map	DSCP to Discard Class Mutation map.
prec1	Precedence in IP(v4) and IPv6 packets.
cos3	IEEE 802.1Q class of service.
precedence-cos-map	Precedence to COS Mutation map.
dscp3	DSCP in IP(v4) and IPv6 packets.
precedence-dscp-map	Precedence to DSCP Mutation map.
precedence-discard-class-map	Precedence to Discard Class Mutation map.
dis-class1	Discard class.
discard-class-cos-map	Discard Class to COS Mutation map.
discard-class-dscp-map	Discard Class to DSCP Mutation map.
discard-class-precedence-map	Discard Class to Precedence Mutation map.

Defaults

None

Command Modes

Policy Map Class Configuration (config-pmap-c-qos)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to set class attributes:

```
n1000v# configure terminal
n1000v(config)# policy-map pm1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# set qos-group 1
```

```
n1000v(config-pmap-c-qos)#
```

This example shows how to remove class attributes:

```
n1000v# configure terminal
n1000v(config)# policy-map pm1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# no set qos-group 1
n1000v(config-pmap-c-qos)#
```

Related Commands

Command	Description
show policy-map	Displays policy maps.

setup

To use the Basic System Configuration Dialog for creating or modifying your system configuration file, use the **setup** command.

setup

Syntax Description

This command has no arguments or keywords, but the Basic System Configuration Dialog prompts you for complete setup information (see the example below).

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The Basic System Configuration Dialog assumes the factory defaults. Keep this in mind when using it to modify an existing configuration.

All changes made to your configuration are summarized for you at the completion of the setup sequence with an option to save the changes or not.

You can exit the setup sequence at any point by pressing Ctrl-C.

Examples

This example shows how to use the setup command to create or modify a basic system configuration:

```
n1000v# setup


  Enter the domain id<1-4095>: 400

  Enter HA role[standalone/primary/secondary]: standalone

[######################################] 100%


          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
```

```
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): y

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : n1000v

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

    Mgmt0 IPv4 address :

  Configure the default gateway? (yes/no) [y]: n

  Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [y]:

  Enable the ssh service? (yes/no) [n]:

  Configure the ntp server? (yes/no) [n]:

  Configure vem feature level? (yes/no) [n]:

  Configure svs domain parameters? (yes/no) [y]:

    Enter SVS Control mode (L2 / L3) : l2
    Invalid SVS Control Mode
    Enter SVS Control mode (L2 / L3) : L2
    Enter control vlan <1-3967, 4048-4093> : 400

    Enter packet vlan <1-3967, 4048-4093> : 405

The following configuration will be applied:
  switchname n1000v
  telnet server enable
  no ssh server enable
  svs-domain
    svs mode L2
    control vlan 400
    packet vlan 405
    domain id 400
vlan 400
vlan 405

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]: n

n1000v#
```

Related Commands

Command	Description
show running-config	Displays the running configuration.

shutdown

To shutdown VLAN switching, use the **shutdown** command. To turn on VLAN switching, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to shutdown VLAN switching:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# shutdown
n1000v(config-vlan)#
```

This example shows how to turn on VLAN switching:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# no shutdown
n1000v(config-vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

sleep

To set a sleep time, use the **sleep** command.

sleep *time*

Syntax Description

time	Sleep time, in seconds. The range of valid values is 0 to 2147483647.

Defaults

Sleep time is not set.

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

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

Usage Guidelines

When you set *time* to 0, sleep is disabled.

Examples

This example shows how to set a sleep time:

```
n1000v# sleep 100
n1000v#
```

This example shows how to disable sleep:

```
n1000v# sleep 0
n1000v#
```

ssh

To create a Secure Shell (SSH) session, use the **ssh** command.

ssh [*username*@]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]

Syntax Description

username	(Optional) Username for the SSH session. The user name is not case sensitive.
ipv4-address	IPv4 address of the remote device.
hostname	Hostname of the remote device. The hostname is case sensitive.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The VRF name is case sensitive.

Defaults

Default VRF

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The NX-OS software supports SSH version 2.

Examples

This example shows how to start an SSH session:

```
n1000v# ssh 10.10.1.1 vrf management
The authenticity of host '10.10.1.1 (10.10.1.1)' can't be established.
RSA key fingerprint is 9b:d9:09:97:f6:40:76:89:05:15:42:6b:12:48:0f:d6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.1.1' (RSA) to the list of known hosts.
User Access Verification
Password:
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
ssh server enable	Enables the SSH server.

ssh key

To create a Secure Shell (SSH) server key for a virtual device context (VDC), use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

Syntax Description

dsa	Specifies the Digital System Algrorithm (DSA) SSH server key.
force	(Optional) Forces the replacement of an SSH key.
rsa	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
length	(Optional) Number of bits to use when creating the SSH server key. The range is from 768 to 2048.

Defaults

1024-bit length

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The NX-OS software supports SSH version 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no ssh server enable** command.

Examples

This example shows how to create an SSH server key using DSA:

```
n1000v# config t
n1000v(config)# ssh key dsa
generating dsa key(1024 bits).....
..
generated dsa key
```

This example shows how to create an SSH server key using RSA with the default key length:

```
n1000v# config t
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
n1000v# config t
n1000v(config)# ssh key rsa 768
generating rsa key(768 bits).....
.
generated rsa key
```

This example shows how to replace an SSH server key using DSA with the force option:

```
n1000v# config t
n1000v(config)# no ssh server enable
n1000v(config)# ssh key dsa force
deleting old dsa key.....
generating dsa key(1024 bits).....
.
generated dsa key
n1000v(config)# ssh server enable
```

This example shows how to remove the DSA SSH server key:

```
n1000v# config t
n1000v(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
n1000v(config)# no ssh key dsa
n1000v(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

```
n1000v# config t
n1000v(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
n1000v(config)# no ssh key
n1000v(config)# ssh server enable
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
ssh server enable	Enables the SSH server.

ssh server enable

To enable the Secure Shell (SSH) server, use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The NX-OS software supports SSH version 2.

Examples

This example shows how to enable the SSH server:

```
n1000v# config t
n1000v(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
n1000v# config t
n1000v(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
```

Related Commands

Command	Description
show ssh server	Displays the SSH server key information.

state (VLAN)

To set the operational state of a VLAN, use the **state** command. To disable state configuration, use the **no** form of this command.

state {**active** | **suspend**}

no state

Syntax Description

active	Specifies the active state.
suspend	Specifies the suspended state.

Defaults

None

Command Modes

VLAN configuration (config-vlan)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to set the operational state of a VLAN:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# state active
n1000v(config-vlan)#
```

This example shows how to disable state configuration:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# no state
n1000v(config-vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

state (Port Profile)

To set the operational state of a port profile, use the **state** command.

state enabled

Syntax Description

enabled	Enables or disables the port profile.

Defaults

Disabled

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to enable or disable the operational state of a port profile:

```
n1000v# configure terminal
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# state enabled
n1000v(config-port-prof)#
```

Related Commands

Command	Description
show port-profile	Displays port profile information.

statistics per-entry

To collect statistics for each ACL entry, use the **statistics per-entry** command. To remove statistics, use the **no** form of this command.

statistics per-entry

no statistics per-entry

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are collected.

Command Modes

ACL configuration (config-acl)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to collect statistics for each ACL entry:

```
n1000v# configure terminal
n1000v(config)# ip access-list 1
n1000v(config-acl)# statistics per-entry
n1000v(config-acl)#
```

This example shows how to remove statistics:

```
n1000v# configure terminal
n1000v(config)# ip access-list 1
n1000v(config-acl)# no statistics per-entry
n1000v(config-acl)#
```

Related Commands

Command	Description
show statistics	Displays statistics.

svs connection

To enable an SVS connection, use the **svs connection** command. To disable an SVS connection, use the **no** form of this command.

svs connection *name*

no svs connection *name*

Syntax Description

name	Connection name.

Defaults

None

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Only one SVS connection can be enabled per session.

Examples

This example shows how to enable an SVS connection:

```
n1000v# configure terminal
n1000v(config)# svs connection conn1
n1000v(config-svs-conn)#
```

This example shows how to disable an SVS connection:

```
n1000v# configure terminal
n1000v(config)# no svs connection conn1
n1000v(config)#
```

Related Commands

Command	Description
show svs	Displays SVS information.

svs-domain

To configure an SVS domain and enter SVS domain configuration mode, use the **svs-domain** command.

svs-domain

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Examples

This example shows how to enter SVS domain configuration mode to configure an SVS domain:

```
n1000v# configure terminal
n1000v(config)# svs-domain
n1000v(config-svs-domain)#
```

Related Commands

Command	Description
show svs	Displays SVS information.

svs license transfer src-vem

To transfer licenses from a specified source VEM to another VEM, or to transfer an unused license to the VSM license pool, use the **svs license transfer src-vem** command.

svs license transfer src-vem *module number* [**dst-vem** *module number* | **license_pool**]

Syntax Description

dst-vem *module-number*	Specifies the VEM to receive the transferred license.
license_pool	Transfers a license back to the VSM license pool.

Defaults

None

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

- Licenses cannot be transferred to a VEM unless there are sufficient licenses in the pool for all CPUs on that VEM.
- When licenses are successfully transferred from one VEM to another, then the following happens:
  - The virtual Ethernet interfaces on the source VEM are removed from service.
  - The virtual Ethernet interfaces on the destination VEM are brought into service.
- When licenses are successfully transferred from a VEM to the VSM license pool, then the following happens:
  - The virtual Ethernet interfaces on the source VEM are removed from service.

Examples

This example shows how to transfer a license from VEM 3 to VEM 5, and then display the license configuration:

```
n1000v# config t
n1000v(config)# svs license transfer src-vem 3 dst-vem 5
n1000v(config)# show license usage NEXUS1000V_LAN_SERVICES_PKG
Application
-----------
VEM 5 - Socket 1
VEM 5 - Socket 2
VEM 4 - Socket 1
VEM 4 - Socket 2
-----------

n1000v#
```

This example shows how to transfer a license from VEM 3 to the VSM license pool, and then display the license configuration:

```
n1000v# config t
n1000v(config)# svs license transfer src-vem 3 license_pool
n1000v(config)# show license usage NEXUS1000V_LAN_SERVICES_PKG
Application
-----------
VEM 4 - Socket 1
VEM 4 - Socket 2
-----------

n1000v#
```

Related Commands

Command	Description
show license usage	Displays the number and location of CPU licenses in use on your VEMs.
logging level license	Designates the level of severity at which license messages should be logged.
install license	Installs a license file(s) on a VSM
svs license transfer src-vem	Transfers licenses from a source VEM to another VEM, or to the VSM pool of available licenses.

svs license volatile

To enable volatile licenses so that, whenever a VEM is taken out of service, its licenses are returned to the VSM pool of available licenses, use the **svs license volatile** command. To disable volatile licenses, use the **no** form of this command.

svs license volatile

no svs license volatile

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Caution **Service Disruption**
Volatile licenses are removed from a VEM during a loss in connectivity and are not returned to the VEM when connectivity resumes. Cisco recommends that the volatile license feature remain disabled and that you, instead, transfer unused licenses using the **svs license transfer src-vem** command.

Examples

This example shows how to enable the volatile license feature for a VSM:

```
n1000v(config)# svs license volatile
n1000v(config)#
```

This example shows how to disable the volatile license feature for a VSM:

```
n1000v(config)# no svs license volatile
```

Related Commands

Command	Description
show license	Displays the license configuration for the VSM.
logging level license	Designates the level of severity at which license messages should be logged.
install license	Installs a license file(s) on a VSM
svs license transfer src-vem	Transfers licenses from a source VEM to another VEM, or to the VSM pool of available licenses.

switchname

To configure the hostname for the device, use the **switchname** command. To revert to the default, use the **no** form of this command.

switchname *name*

no switchname

Syntax Description

name	Name for the device. The name is alphanumeric, case sensitive, can contain special characters, and can have a maximum of 32 characters.

Defaults

switch

Command Modes

Global Configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The Cisco NX-OS software uses the hostname in command-line interface (CLI) prompts and in default configuration filenames.

The **switchname** command performs the same function as the **hostname** command.

Examples

This example shows how to configure the device hostname:

```
n1000v# configure terminal
n1000v(config)# switchname Engineering2
Engineering2(config)#
```

This example shows how to revert to the default device hostname:

```
Engineering2# configure terminal
Engineering2(config)# no switchname
n1000v(config)#
```

Related Commands

Command	Description
hostname	Configures the device hostname.
show switchname	Displays the device hostname.

switchport access vlan

To set the access mode of an interface, use the **switchport access vlan** command. To remove access mode configuration, use the **no** form of this command.

switchport access vlan *id*

no switchport access vlan

Syntax Description

id	VLAN identification number. The range of valid values is 1 to 3967.

Defaults

Access mode is not set.

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to set the access mode of an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# switchport access vlan 10
n1000v(config-if)#
```

This example shows how to remove access mode configuration:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# no switchport access vlan
n1000v(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface information.

switchport mode

To set the port mode of an interface, use the **switchport mode** command. To remove the port mode configuration, use the **no** form of this command.

switchport mode {access | private-vlan {host | promiscuous} | trunk}

no switchport mode {access | private-vlan {host | promiscuous} | trunk}

Syntax Description

access	Sets port mode access.
private-vlan	Sets the port mode to private VLAN.
host	Sets the port mode private VLAN to host.
promiscuous	Sets the port mode private VLAN to promiscuous.
trunk	Sets the port mode to trunk.

Defaults

Switchport mode is not set.

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to set the port mode of an interfn1000vace:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# switchport mode private-vlan host
n1000v(config-if)#
```

This example shows how to remove mode configuration:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# no switchport mode private-vlan host
n1000v(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface information.

switchport port-security

To set the port security characteristics of an interface, use the **switchport port-security** command. To remove the port security configuration, use the **no** form of this command.

switchport port-security [aging {time *time* **| type {absolute | inactivity}} | mac-address {***address* **[vlan** *id***] |sticky} | maximum** *number* **[vlan** *id***] | violation {protect | shutdown}]**

no switchport port-security [aging {time *time* **| type {absolute | inactivity}} | mac-address {***address* **[vlan** *id***] |sticky} | maximum** *number* **[vlan** *id***] | violation {protect | shutdown}]}**

Syntax Description

aging	Configures port security aging characteristics.
time	Specifies the port security aging time.
time	Aging time in minutes, in the range of 0 to 1440.
type	Specifies the type of timers.
absolute	Specifies an absolute timer.
inactivity	Specifies an inactivity timer.
mac-address *address*	Specifies a 48-bit MAC address in the format *HHHH.HHHH.HHHH*.
vlan	Specifies the VLAN where the MAC address should be secured.
id	VLAN identification number. The range of valid values is 1 to 4094.
sticky	Specifies a sticky MAC address.
maximum *number*	Specifies the maximum number of addresses, in the range of 1 to 1025.
violation	Specifies the security violation mode.
protect	Specifies the security violation protect mode.
shutdown	Specifies the security violation shutdown mode.

Defaults

None

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to set the port security aging inactivity timer:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# switchport port-security aging type inactivity
n1000v(config-if)#
```

This example shows how to remove the port security aging inactivity timer:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# no switchport port-security aging type inactivity
n1000v(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface information.
show port-security	Displays port security information.

switchport private-vlan host-association

To define a private VLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the private VLAN association from the port, use the **no** form of this command.

switchport private-vlan host-association {*primary-vlan-id*} {*secondary-vlan-id*}

no switchport private-vlan host-association

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship.

Defaults

None

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-host mode. If the port is in private VLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive. The port also may be inactive when the association between the private VLANs is suspended.

The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure a host private VLAN port with a primary VLAN (VLAN 18) and a secondary VLAN (VLAN 20):

```
n1000v(config-if)# switchport private-vlan host-association 18 20
n1000v(config-if)#
```

This example shows how to remove the private VLAN association from the port:

```
n1000v(config-if)# no switchport private-vlan host-association
n1000v(config-if)#
```

Related Commands

Command	Description
show vlan private-vlan [type]	Displays information on private VLANs.

switchport private-vlan mapping

To define the private VLAN association for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mapping from the primary VLAN, use the **no** form of this command.

switchport private-vlan mapping {*primary-vlan-id*} {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}

no switchport private-vlan mapping

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
add	Associates the secondary VLANs to the primary VLAN.
secondary-vlan-list	Number of the secondary VLAN of the private VLAN relationship.
remove	Clears the association between the secondary VLANs and the primary VLAN.

Defaults

None

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-promiscuous mode. If the port is in private VLAN-promiscuous mode but the primary VLAN does not exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure the associate primary VLAN 18 to secondary isolated VLAN 20 on a private VLAN promiscuous port:

```
n1000v(config-if)# switchport private-vlan mapping 18 20
n1000v(config-if)#
```

This example shows how to add a VLAN to the association on the promiscuous port:

```
n1000v(config-if)# switchport private-vlan mapping 18 add 21
n1000v(config-if)#
```

This example shows how to remove the all private VLAN association from the port:

```
n1000v(config-if)# no switchport private-vlan mapping
n1000v(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays information on all interfaces configured as switchports.
show interface private-vlan mapping	Displays the information about the private VLAN mapping for VLAN interfaces, or SVIs.

switchport private-vlan mapping trunk

To designate the primary private VLAN, use the **switchport private-vlan trunk mapping trunk** command. To remove the primary private VLAN, use the **no** form of this command.

switchport private-vlan trunk native vlan *id*

no switchport private-vlan trunk native vlan

Syntax Description

id	VLAN identification number. The range of valid values is 1 to 3967.

Defaults

None

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

When you use this command, you must either add a secondary VLAN, or remove a VLAN.

Examples

This example shows how to designate the primary private VLAN:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# n1000v(config-if)# switchport private-vlan mapping trunk 10 add 11
n1000v(config-if)#
```

This example shows how to remove the primary private VLAN:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# n1000v(config-if)# no switchport private-vlan mapping trunk 10
n1000v(config-if)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

switchport trunk allowed vlan

To set the list of allowed VLANs on the trunking interface, use the **switchport trunk allowed vlan** command. To allow *all* VLANs on the trunking interface, use the **no** form of this command.

switchport trunk allowed vlan {*vlan-list* | **all** | **none** | [**add** | **except** | **remove** {*vlan-list*}]}

no switchport trunk allowed vlan

Syntax Description

vlan-list	Allowed VLANs that transmit through this interface in tagged format when in trunking mode; the range of valid values is from 1 to 4094.
all	Allows all appropriate VLANs to transmit through this interface in tagged format when in trunking mode.
none	Blocks all VLANs transmitting through this interface in tagged format when in trunking mode.
add	(Optional) Adds the defined list of VLANs to those currently set instead of replacing the list.
except	(Optional) Allows all VLANs to transmit through this interface in tagged format when in trunking mode except the specified values.
remove	(Optional) Removes the defined list of VLANs from those currently set instead of replacing the list.

Defaults

All VLANs

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport trunk allowed vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic in VLAN 1.

Examples

This example shows how to add a series of consecutive VLANs to the list of allowed VLANs on a trunking port:

```
n1000v(config-if)# switchport trunk allowed vlan add 40-50
n1000v(config-if)#
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport trunk native vlan

To configure trunking parameters on an interface, use the **switchport trunk native vlan** command. To remove the configuration, use the **no** form of this command.

switchport trunk native vlan *id*

no switchport trunk native vlan

Syntax Description

id	VLAN identification number. The range of valid values is 1 to 3967.

Defaults

None

Command Modes

Interface Configuration (config-if)
Port Profile Configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to configure trunking parameters on an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 10
n1000v(config-if)# switchport trunk native vlan 20
n1000v(config-if)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

system redundancy role

To configure a redundancy role for the VSM, use the **system redundancy role** command. To revert to the default setting, use the **no** form of the command.

system redundancy role {primary | secondary | standalone}

no system redundancy role {primary | secondary | standalone}

Syntax Description

primary	Specifies the primary redundant VSM.
secondary	Specifies the secondary redundant VSM.
standalone	Specifies no redundant VSM.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Examples

This example shows how to configure no redundant VSM:

```
n1000v# system redundancy role standalone
n1000v#
```

Related Commands

Command	Description
show system redundancy	Displays the system redundancy status.

system switchover

To switch over to the standby supervisor, use the **system switchover** command.

system switchover

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Examples

This example shows how to switch over to the standby supervisor:

```
n1000v# system switchover
n1000v#
```

Related Commands

Command	Description
show system redundancy	Displays the system redundancy status.