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.

server

To configure the RADIUS server as a member of the RADIUS server group, use the **server** command. To remove a server, use the **no** form of this command.

server {*ipv4-address* | *server-name*}

no server {*ipv4-address* | *server-name*}

Syntax Description

ipv4-address	IPV4 address of the RADIUS server.
server-name	Name that identifies the RADIUS server.

Defaults

None

Command Modes

Radius configuration (config-radius)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to configure the RADIUS server as a member of the RADIUS server group:

```
n1000v# config t
n1000v(config)# aaa group server radius RadServer
n1000v(config-radius)# server 10.10.1.1
n1000v(config-radius)#
```

This example shows how to remove the server configuration:

```
n1000v# config t
n1000v(config)# aaa group server radius RadServer
n1000v(config)# no server 10.10.1.1
```

Related Commands

Command	Description
aaa group server radius	Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group.
deadtime	Configures the monitoring dead time.
use-vrf	Specifies the Virtual Routing and Forwarding (VRF) to use to contact the servers in the server group.
show radius-server groups	Displays the RADIUS server group configuration.

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.

service-port

To configure an inside or outside interface in a virtual service domain (VSD) port profile, use the **service-port** command. To remove the configuration, use the **no** form of this command.

service-port {**inside** | **outside**} **default-action** {**drop** | **forward**}

no service-port

Syntax Description

inside	Inside Network
outside	Outside Network
default-action	Action to be taken if service port is down. • **drop**: drops packets • **forward**: forwards packets

Defaults

None

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

If a port profile without a service port is configured on an SVM, it will flood the network with packets.

When configuring a port profile on an SVM, first bring the SVM down, This prevents a port-profile that is mistakenly configured without a service port from flooding the network with packets. The SVM can be returned to service after the configuration is complete and verified.

The **service-port** command is configurable only after the port-profile is configured for trunk mode and the virtual-service-domain has been configured.

Caution You should not add packet and control VLANs to the allowed VLAN list of a port-profile that has the service port configured. This causes a loop.

Examples

This example shows how to configure an inside interface on a VSD port profile that drops packets if the service port is down:

```
n1000v# config t
n1000v(config)# port-profile svm_vsd1_in
```

```
n1000v(config-port-prof)# switchport mode trunk
n1000v(config-port-prof)# virtual-service-domain test
n1000v(config-port-prof)# service-port inside default-action drop
n1000v(config-port-prof)#
```

This example shows how to remove a service port configuration:

```
n1000v# config t
n1000v(config)# port-profile svm_vsd1_in
n1000v(config-port-prof)# no service-port
n1000v(config-port-prof)#
```

Related Commands

Command	Description
show virtual-service-domain brief	Displays a list of the VSDs currently configured in a VSM, including VSD names and port profiles.
show virtual-service-domain interface	Displays a list of currently assigned interfaces to the VSDs in a VSM.
show virtual-service-domain name	Displays a specific VSD currently configured in a VSM.

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)#
```

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 a 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#
```

snmp-server aaa-user cache-timeout

To configure how long the AAA-synchronized user configuration stays in the local cache, use the **snmp-server aaa-user cache-timeout** command. To revert back to the default value of 3600 seconds, use the **no** form of this command.

snmp-server user aaa-user cache-timeout *seconds*

no snmp-server user aaa-user cache-timeout *seconds*

Syntax Description

seconds	Length of the time for the user configuration to remain in the local cache. The range is 1 to 86400 seconds.

Defaults

The default timeout is 3600 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 AAA-synchronized user configuration to stay in the local cache for 1200 seconds:

```
n1000v# config t
n1000v(config)# snmp-server aaa-user cache-timeout 1200
```

This example shows how to revert back to the default value of 3600 seconds:

```
n1000v# config t
n1000v(config)# no snmp-server aaa-user cache-timeout 1200
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server contact	Configures sysContact, (the SNMP contact).
snmp-server protocol enable	Enables the SNMP protocol.
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server location	Configures sysLocation (the SNMP location).

Command	Description
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.
snmp-server user	Configures an SNMP user with authentication and privacy parameters.

snmp-server community

To create an SNMP community string and assign access privileges for the community, use the **snmp-server community** command.

To remove the community or its access privileges, use the **no** form of this command.

snmp-server community *string* [**group** *group-name*] [**ro** | **rw**]

no snmp-server community *string* [**group** *group-name*] [**ro** | **rw**]

Syntax Description

string	SNMP community string, which identifies the community.
group	(Optional) Specifies a group to which this community belongs.
group-name	Name that identifies an existing group.
ro	(Optional) Specifies read-only access for this community.
rw	(Optional) Specifies read-write access for this community.

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

You can create SNMP communities for SNMPv1 or SNMPv2c.

Examples

This example shows how to configure read-only access for the SNMP community called public:

```
n1000v# config t
n1000v(config)# snmp-server community public ro
```

This example shows how to remove the SNMP community called public:

```
n1000v# config t
n1000v(config)# no snmp-server community public
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server contact	Configures sysContact, (the SNMP contact).
snmp-server protocol enable	Enables SNMP.
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server location	Configures sysLocation (the SNMP location).
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.
snmp-server user	Configures an SNMP user with authentication and privacy parameters.
snmp-server community	Creates an SNMP community string and assigns access privileges for the community.

snmp-server contact

To configure the sysContact, which is the SNMP contact name, use the **snmp-server contact** command.

To remove or modify the sysContact, use the **no** form of this command.

snmp-server contact [*name*]

no snmp-server contact [*name*]

Syntax Description

name	(Optional) SNMP contact name (sysContact), which can contain a maximum of 32 characters.

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

You can create SNMP communities for SNMPv1 or SNMPv2c.

Examples

This example shows how to configure the sysContact to be Admin:

```
n1000v# config t
n1000v(config)# snmp-server contact Admin
```

This example shows how to remove the sysContact:

```
n1000v# config t
n1000v(config)# no snmp-server contact
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server protocol enable	Enables SNMP.

Command	Description
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server location	Configures sysLocation (the SNMP location).
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.
snmp-server user	Configures an SNMP user with authentication and privacy parameters.

snmp-server globalEnforcePriv

To enforce SNMP message encryption for all users, use the **snmp-server globalEnforcePriv** command.

snmp-server globalEnforcePriv

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to enforce SNMP message encryption for all users:

```
n1000v# config t
n1000v(config)# snmp-server mib globalEnforcePriv
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server contact	Configures sysContact, (the SNMP contact).
snmp-server protocol enable	Enables SNMP.
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server location	Configures sysLocation (the SNMP location).
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.
snmp-server user	Configures an SNMP user with authentication and privacy parameters.

snmp-server host

To configure a host receiver for SNMPv1 or SNMPv2c traps, use the **snmp-server host** command. To remove the host, use the **no** form of this command.

snmp-server host *ip-address* {**traps** | **informs**}{**version** {**1** | **2c** | **3**}} [**auth** | **noauth** | **priv**] *community* [**udp_port** *number*]

no snmp-server host *ip-address* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} [**auth** | **noauth** | **priv**] *community* [**udp_port** *number*]

Syntax Description

ip-address	IPv4 address, IPv6 address, or DNS name of the SNMP notification host.
informs	Specifies Inform messages to this host.
traps	Specifies Traps messages to this host.
version	Specifies the SNMP version to use for notification messages.
1	Specifies SNMPv1 as the version.
2c	Specifies SNMPv2c as the version.
3	Specifies SNMPv3 as the version.
auth	(Optional) Specifies (for SNMPv3) the authNoPriv Security Level.
noauth	(Optional) Specifies (for SNMPv3) the noAuthNoPriv Security Level.
priv	(Optional) Specifies (for SNMPv3) the authPriv Security Level.
community	SNMPv1/v2c community string or SNMPv3 user name. The community string can be any alphanumeric string up to 255 characters.
udp-port	(Optional) Specifies an existing UDP port.
number	Number that identifies the UDP port of the notification host. The range is 0 to 65535.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

This example shows how to configure the host receiver, 192.0.2.1, for SNMPv1 traps:

```
n1000v# config t
n1000v(config)# snmp-server host 192.0.2.1 traps version 1 public
```

This example shows how to remove the configuration:

```
n1000v# config t
n1000v(config)# no snmp-server host 192.0.2.1 traps version 1 public
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server contact	Configures sysContact, (the SNMP contact).
snmp-server protocol enable	Enables SNMP.
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
snmp-server location	Configures sysLocation (the SNMP location).
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.
snmp-server user	Configures an SNMP user with authentication and privacy parameters.

snmp-server location

To configure the sysLocation, which is the SNMP location name, use the **snmp-server location** command.

To remove the sysLocation, use the **no** form of this command.

snmp-server location [*name*]

no snmp-server location [*name*]

Syntax Description

name	(Optional) SNMP location name (sysLocation), which can contain a maximum of 32 characters.

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 sysLocation to be Lab-7:

```
n1000v# config t
n1000v(config)# snmp-server location Lab-7
```

This example shows how to remove the sysLocation:

```
n1000v# config t
n1000v(config)# no snmp-server location
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server contact	Configures sysContact (the SNMP contact).
snmp-server protocol enable	Enables SNMP.
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.

Command	Description
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.
snmp-server user	Configures an SNMP user with authentication and privacy parameters.

snmp-server protocol enable

To enable SNMP protocol operations, use the **snmp-server protocol enable** command. To disable SNMP protocol operations, use the **no** form of this command.

snmp-server protocol enable

no snmp-server protocol enable

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to enable SNMP protocol operations:

```
n1000v# config t
n1000v(config)# snmp-server protocol enable
```

This example shows how to disable SNMP protocol operations:

```
n1000v# config t
n1000v(config)# no snmp-server protocol enable
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server contact	Configures sysContact (the SNMP contact).
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server location	Configures sysLocation (the SNMP location).

Command	Description
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.
snmp-server user	Configures an SNMP user with authentication and privacy parameters.

snmp-server tcp-session

To enable authentication for SNMP over TCP, use the **snmp-server tcp-session** command. To disable authentication for SNMP over TCP, use the **no** form of this command.

snmp-server tcp-session [**auth**]

no snmp-server tcp-session

Syntax Description

auth	(Optional) Enables one-time authentication for SNMP over the entire TCP session (rather than on a per-command basis).

Defaults

This command is disabled by default.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to enable one-time authentication for SNMP over TCP:

```
n1000v# config t
n1000v(config)# snmp-server tcp-session auth
```

This example shows how to disable one-time authentication for SNMP over TCP:

```
n1000v# config t
n1000v(config)# no snmp-server tcp-session
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server contact	Configures sysContact, (the SNMP contact).
snmp-server protocol enable	Enables SNMP.
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server location	Configures sysLocation (the SNMP location).
snmp-server user	Configures an SNMP user with authentication and privacy parameters.

snmp-server user

To define a user who can access the SNMP engine, use the **snmp-server user** command. To deny a user access to the SNMP engine, use the **no** form of this command.

snmp-server user *name* [**auth** {**md5** | **sha**} *passphrase-1* [**priv** [**aes-128**] *passphrase-2*] [**engineID** *id*] [**localizedkey**]]

no snmp-server user *name*

Syntax Description

name	Name of a user who can access the SNMP engine.
auth	(Optional) Enables one-time authentication for SNMP over a TCP session
md5	(Optional) Specifies HMAC MD5 algorithm for authentication.
sha	(Optional) Specifies HMAC SHA algorithm for authentication.
passphrase-1	Authentication passphrase for this user. The passphrase can be any case-sensitive alphanumeric string up to 64 characters.
priv	(Optional) Specifies encryption parameters for the user.
aes-128	(Optional) Specifies a 128-byte AES algorithm for privacy.
passphrase-2	Encryption passphrase for this user. The passphrase can be any case-sensitive alphanumeric string up to 64 characters.
engineID	(Optional) Specifies the engineID for configuring the notification target user (for V3 informs).
id	Number that identifies the engineID, in a 12-digit, colon-separated decimal format.
localizedkey	(Optional) Specifies the passphrase as any case-sensitive alphanumeric string up to 130 characters.

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 provide one-time SNMP authorization for the user, Admin, using the HMAC SHA algorithm for authentication:

```
n1000v# config t
n1000v(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

This example shows how to deny a user access to the SNMP engine:

```
n1000v# config t
n1000v(config)# no snmp-server user Admin
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server aaa-user cache-timeout	Configures how long the AAA-synchronized user configuration stays in the local cache.
snmp-server contact	Configures sysContact (the SNMP contact).
snmp-server protocol enable	Enables SNMP.
snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
snmp-server host	Configures a host receiver for SNMP traps or informs.
snmp-server location	Configures sysLocation (the SNMP location).
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.

snmp trap link-status

To enable SNMP link-state traps for the interface, use the **snmp trap link-status** command. To disable SNMP link-state traps for the interface, use the **no** form of this command.

snmp trap link-status

no snmp trap link-status

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

CLI interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

This command is enabled by default.

Examples

This example shows how to enable SNMP link-state traps for the interface:

```
n1000v# config t
n1000v(config)# interface veth 2
n1000v(config-if)# snmp trap link-status
n1000v(config-if)#
```

This example shows how to disable SNMP link-state traps for the interface:

```
n1000v# config t
n1000v(config)# interface veth 2
n1000v(config-if)# no snmp trap link-status
n1000v(config-if)#
```

Related Commands

Command	Description
interface vethernet	Creates a virtual Ethernet interface and enters interface configuration mode.
snmp-server enable traps	Enables all SNMP notifications.
snmp-server tcp-session	Enables a one-time authentication for SNMP over a TCP session.

source mgmt (NetFlow)

To add an interface to a flow exporter designating it as the source for NetFlow flow records, use the **source** command. To remove the source interface from the flow exporter, use the **no** form of this command.

source mgmt *0*

no source

Syntax Description

mgmt 0	Adds the mgmt 0 interface to the flow exporter.

Defaults

None

Command Modes

NetFlow flow exporter configuration (config-flow-exporter)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The mgmt0 interface is the only interface that can be added to the flow exporter.

Examples

This example shows how to add source management interface 0 to the ExportTest flow exporter:

```
n1000v(config)# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# source mgmt 0
```

This example shows how to remove source management interface 0 from the ExportTest flow exporter:

```
n1000v(config)# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no source mgmt 0
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow record	Creates a Flexible NetFlow flow record.
flow monitor	Creates a Flexible NetFlow flow monitor.
show flow exporter	Displays information about the NetFlow flow exporter.

Command	Description
show flow record	Displays information about NetFlow flow records.
show flow monitor	Displays information about the NetFlow flow monitor.

speed

To set the speed for an interface, use the **speed** command. To automatically set both the speed and duplex parameters to auto, use the **no** form of this command.

speed {*speed_val* | **auto** [**10 100** [**1000**]]}

no speed [{*speed_val* | **auto** [**10 100** [**1000**]]}]

Syntax Description

speed_val	Port speed on the interface, in Mbps.
auto	Sets the interface to autonegotiate the speed with the connecting port.
10	(Optional) Specifies a speed of 10 Mbps.
100	(Optional) Specifies a speed of 100 Mbps.
1000	(Optional) Specifies a speed of 1000 Mbps.

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

If you configure an Ethernet port speed to a value other than auto (for example, 10, 100, or 1000 Mbps), you must configure the connecting port to match. Do not configure the connecting port to negotiate the speed.

Examples

This example shows how to set the speed of Ethernet port 1 on the module in slot 3 to 1000 Mbps:

```
n1000v config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)# speed 1000
```

This example shows how to automatically set the speed to auto:

```
n1000v config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)# no speed 1000
```

Related Commands

Command	Description
interface	Specifies the interface that you are configuring.
duplex	Specifies the duplex mode as full, half, or autonegotiate.
show interface	Displays the interface status, which includes the speed and duplex mode parameters.

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 generate the key pair for the switch, which is used if SSH server is enabled, 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.

sub-group

To configure interface port channel subgroup assignment, use the **sub-group** command. To remove this configuration, use the **no** form of this command.

sub-group {**cdp** | **manual**}

no sub-group

Syntax Description

cdp	Specifies that Cisco Discovery Protocol (CDP) information is used to automatically create subgroups for managing the traffic flow.
manual	Specifies that subgroups are configured manually. This option is used if CDP is not configured on the upstream switches.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0	This command was introduced.
4.0(4)SV1(2)	The **manual** keyword was added.

Usage Guidelines

Use this command to identify the port channel as being in vPC-HM, which requires traffic to be managed separately for each upstream switch connected to the member ports. If the upstream switches have CDP enabled, the Cisco Nexus 1000V can use this information to automatically assign subgroups. If the upstream swiches do not have CDP enabled, then you must configure subgroups manually.

This command overrides any subgroup configuration specified in the port-profile inherited by the port channel interface.

Examples

This example shows how to configure a subgroup type for a port channel interface:

```
h1000v# config t
n1000v(config)# interface port-channel 1
n1000v(config-if)# sub-group cdp
```

This example shows how to remove the configuration:

```
h1000v# config t
n1000v(config)# interface port-channel 1
n1000v(config-if)# no sub-group
```

Related Commands

Command	Description
show interface port channel *channel-number*	Displays port-channel information.

sub-group-id

To configure subgroup IDs for Ethernet member ports of vPC-HM, use the **sub-group-id** command. To remove the subgroup IDs, use the **no** form of this command.

sub-group-id *group_id*

no sub-group-id

Syntax Description

group_id	Subgroup ID number. Range is from 0 to 31.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0	This command was introduced.
4.0(4)SV1(2)	The number of subgroups was increased to 32.

Examples

This example shows how to configure an Ethernet member port on subgroup 5:

```
n1000v# config t
n1000v(config)# interface Ethernet 3/2
n1000v(config-if)# sub-group-id 1
```

This example shows how to remove the configuration:

```
n1000v# config t
n1000v(config)# interface Ethernet 3/2
n1000v(config-if)# no sub-group-id
```

Related Commands

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

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.

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.

svs mode

To configure a transport mode for control and packet traffic in the virtual supervisor module (VSM) domain, use the **svs mode** command.

svs mode {**L2** | **L3 interface** {**mgmt0** | **control0**}}

Syntax Description

L2	Specifies Layer 2 as the transport mode for the VSM domain.
L3 interface	Specifies Layer 3 as the transport mode for the VSM domain and configures the Layer 3 transport interface.
mgmt0	Specifies mgmt0 as the Layer 3 transport interface.
control0	Specifies control0 as the Layer 3 transport interface.

Defaults

Layer 2 mode

Command Modes

SVS domain configuration (config-svs-domain)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

If you use mgmt0 as the Layer 3 control interface, then in the VSM VM, Ethernet adapters 1 and 3 are not used.

If you use control0 as the Layer 3 control interface, then in the VSM VM, Ethernet adapter 3 is not used.

Examples

This example shows how to configure mgmt0 as the Layer 3 transport interface for the VSM domain:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# svs mode l3 interface mgmt0
n1000v(config-svs-domain)#
```

Related Commands

Command	Description
show svs-domain	Displays the VSM domain configuration.
svs-domain	Creates and configures the VSM domain.

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 interface:

```
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 mapping trunk *primary-vlan* [{**add** | **remove**}] *secondary_vlans*

no switchport private-vlan mapping trunk [*primary-vlan* [*secondary_vlans*]]

Syntax Description

primary-vlan	Primary private VLAN.
add	Add a VLAN to private VLAN list.
remove	Remove a VLAN from private VLAN list.
secondary_vlans	Secondary VLAN IDs.

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)# 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 jumbomtu

To configure a system-wide jumbo frame size, specifying the maximum frame size that Ethernet ports can process, use the **system jumbomtu** command.

system jumbomtu *size*

Syntax Description

size	Size, in bytes, of the Layer 2 Ethernet interface jumbo maximum transmission unit (MTU). Frames larger than this are dropped. The setting must be an even number between 1500 and 9000 bytes.

Defaults

9000 bytes

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

- For transmissions to occur between two ports, you must configure the same MTU size for both ports.
- A port drops any frames that exceed its MTU size.
- If you do not configure a system jumbo MTU size, it defaults to 1500 bytes.
- For a Layer 2 port, you can configure an MTU size as the system default of 1500 bytes or the system default jumbo MTU size of 9000 bytes.
- If you change the system jumbo MTU size, Layer 2 ports automatically use the system default MTU size of 1500 bytes unless you specifically configure the MTU size differently per port.

Examples

This example shows how to configure a system-wide maximum frame size of 8000 bytes:

```
n1000v# config t
n1000v(config)# system jumbomtu 8000
n1000v#
```

Related Commands

Command	Description
show interface ethernet	Displays information about Ethernet interfaces, including the configured MTU size.
show running-config	Displays the current operating configuration, which includes the system jumbo MTU size.

Command	Description
interface ethernet	Specifies an interface to configure and enters interface configuration mode.
mtu	Specifies the system jumbo MTU size.

system mtu

To override any maximum transmission unit (MTU) setting that has already been set on the uplink using the **mtu** command on the interface, use the **system mtu** command. To reset the switch to the default of 1500 for all the ports inheriting this system profile, use the no form of this command.

system mtu *size*

no system mtu

Syntax Description

size	Size, in bytes, of the Layer 2 Ethernet interface maximum transmission unit (MTU). The range is 1500 to 9000, even numbers only.

Defaults

1500 bytes

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(3)	This command was introduced.

Usage Guidelines

The **system mtu** command is only applicable, and the configuration is only effective, for system uplink profiles. The value that is configured for **system mtu** command must be less then value configured in the **system jumbomtu** command.

Configuring the system MTU value on the system port-profile causes the interface inheriting this port-profile to flap. If the system port-profile includes the control VLAN, then the module, itself, will flap.

Examples

This en1000vxample shows how to configure the system MTU value as 3000 bytes for the system uplink profile called PP1:

```
n1000v# config t
n1000v(config-port-prof)# port-profile PP1
n1000v# system mtu 3000
n1000v#
```

Related Commands

Command	Description
show interface ethernet	Displays information about Ethernet interfaces, including the configured MTU size.
show running-config	Displays the current operating configuration, which includes the system jumbo MTU size.
port-profile	Creates a port profile and enters port-profile configuration mode.
mtu	Specifies the system jumbo MTU size.

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.

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.

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.

system update vem feature level

To change the software version supported on VEMs, use the **system update vem feature level** command.

system update vem feature level [*version_number*]

Syntax Description

version_number	(Optional) version number index from the list above.

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 change the software version supported:

```
n1000v# system update vem feature level
Error : the feature level is set to the highest value possible
n1000v#
```

Related Commands

Command	Description
show system vem feature level	Displays the current software release supported.

system vlan

To add the system VLAN to a port profile, use the **system vlan** command. To remove the system VLAN from a port profile, use the **no** form of this command.

system vlan *vlan-ID-list*

no system vlan

Syntax Description

vlan-ID-list	List of VLAN IDs, separated by commas. The allowable range is 1–3967 and 4048–4093.

Defaults

None

Command Modes

Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

A system VLAN is used to configure and bring up physical or vEthernet ports before the Virtual Supervisor Module (VSM) has established communication with the Virtual Ethernet Module (VEM).

Examples

This example shows how to add system VLANs 260 and 261 to the port profile:

```
n1000v# config t
n1000v (config)# port-profile system-uplink
n1000v(config-port-prof)# system vlan 260, 261
n1000v(config-port-prof)#
```

This example shows how to remove all system VLANs from the port profile:

```
n1000v# config t
n1000v (config)# port-profile system-uplink
n1000v(config-port-prof)# no system vlan
n1000v(config-port-prof)#
```

Related Commands

Command	Description
vlan	Creates a VLAN and enters the VLAN configuration mode.
show vlan all-ports	Displays the status of all VLANs and the ports that are configured on them.
show vlan private-vlan	Displays private VLAN information.
show vlan summary	Displays VLAN summary information.