



## S Commands

---

This chapter describes the Cisco Nexus Cloud Services Platform commands that begin with the letter S.

# session-limit

To limit the number of Vegas shell (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*

<b>Syntax Description</b>	<i>number</i>	Number of VSH sessions. The range of valid values is from 1 to 64.
---------------------------	---------------	--

<b>Defaults</b>	No limit is set.
-----------------	------------------

<b>Command Modes</b>	Line configuration (config-line)
----------------------	----------------------------------

<b>SupportedUserRoles</b>	network-admin
---------------------------	---------------

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

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

```
n1010# configure terminal
n1010(config)# line vty
n1010(config-line)# session-limit 10
n1010(config-line)#
```

This example shows how to remove the limit:

```
n1010# configure terminal
n1010(config)# line vty
n1010(config-line)# no session-limit 10
n1010(config-line)#
```

Related Commands	Command	Description
	<b>exec-timeout</b>	Configures the length of time, in minutes, that an inactive Telnet or SSH session remains open before it is automatically shut down.
	<b>line-vty</b>	Enters line configuration mode.

# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

**Usage Guidelines** While the **setup** command contains no arguments or keywords, the Basic System Configuration Dialog prompts you for complete setup information, as shown in the Examples section.

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:

```
n1010# setup

Enter HA role[primary/secondary]: primary

Enter network-uplink type <1-4>:
  1. Ports 1-2 carry all management, control and data vlans
  2. Ports 1-2 management and control, ports 3-6 data
  3. Ports 1-2 management, ports 3-6 control and data
  4. Ports 1-2 management, ports 3-4 control, ports 5-6 data
2

Enter control vlan <1-3967, 4048-4093>: 1
```

```

Enter the domain id<1-4095>: 2801

Enter management vlan <1-3967, 4048-4093>: 1

Error: There was an error executing atleast one of the command
Please verify the following log for the command execution errors.
ERROR: CLI error: Domain id can be configured only once
Warning! Mandatory reload needed for change to take effect.
Save configuration before reload, else Nexus1010 HA will break!

[#####] 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]:

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

Enter the VSA name [Nexus1010]:

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

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]:

The following configuration will be applied:
switchname Nexus1010
telnet server enable
no ssh server enable

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

n1010#

```

**Related Commands**

Command	Description
<b>show running-config</b>	Displays the running configuration.

# shutdown

To disable an interface, use the **shutdown** command. To enable an interface, use the no form of this command.

**shutdown**

**[no] shutdown**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** Interface Configuration (config-if)

**SupportedUserRoles** network-admin

Command History	Release	Modification
	4.2(1)SP1(3)	This command was introduced.

## Usage Guidelines

**Examples** This example shows how to disable VsbEthernet interface 1/1:

```
n1010# configure terminal
n1010(config) interface vsbEthernet 1/1
n1010(config-if) shutdown
```

Related Commands	Command	Description
	<b>interface VsbEthernet</b>	Configures the virtual service blade (VSB) Ethernet interface.
	<b>show virtual-service-blade summary</b>	Displays summary information about all virtual services, such as their role, state, and module.
	<b>virtual-service-blade</b>	Places you into the configuration mode for the named virtual service.

# system shutdown

To shut down the Cisco Nexus Cloud Services Platform (CSP), use the system **shutdown** command. To return the Cisco Nexus Cloud Services Platform status to powered on, use the **no** version of this command.

**system shutdown** [**primary** | **secondary**]

**no system shutdown** [**primary** | **secondary**]

Syntax Description	
<b>primary</b>	(Optional) Specifies only the primary CSP for shutdown.
<b>secondary</b>	(Optional) Specifies only the secondary CSP for shutdown.

Defaults	
	None

Command Modes	
	Global configuration (config)

SupportedUserRoles	
	network-admin network-operator

Command History	Release	Modification
	5.2(1)SP1(7.1)	This command was introduced.

Examples	
	<p>This example shows how to shut down the primary Cisco Nexus Cloud Services Platform:</p> <pre>switch# system shutdown This command will shut down the both the Primary and Secondary Nexus1010. Make sure you save your configuration before proceeding. Do you really want to proceed(yes/no)? [no]</pre>

Related Commands	
	None

# sleep

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

**sleep** *time*

<b>Syntax Description</b>	<i>time</i>	Sleep time, in seconds. The range is from 0 to 2147483647.
---------------------------	-------------	--

<b>Defaults</b>	Sleep time is not set.
-----------------	------------------------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator
---------------------------	-----------------------------------

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

<b>Usage Guidelines</b>	When you set <i>time</i> to 0, sleep is disabled.
-------------------------	---

<b>Examples</b>	This example shows how to set a sleep time:
-----------------	---

```
n1010# sleep 100
n1010#
```

This example shows how to disable sleep:

```
n1010# sleep 0
n1010#
```

## 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*

<b>Syntax Description</b>	<i>seconds</i>	Length of the time for the user configuration to remain in the local cache. The range is from 1 to 86400 seconds.
---------------------------	----------------	---

**Defaults** The default timeout is 3600 seconds.

**Command Modes** Global configuration (config)

**SupportedUserRoles** network-admin

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(4)SP1(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:

```
n1010# configure terminal
n1010(config)# snmp-server aaa-user cache-timeout 1200
```

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

```
n1010# configure terminal
n1010(config)# no snmp-server aaa-user cache-timeout 1200
```

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



Command	Description
<b>snmp-server tcp-session</b>	Enables a one-time authentication for SNMP over a TCP session.
<b>snmp-server user</b>	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	
<i>string</i>	SNMP community string, which identifies the community.
<b>group</b>	(Optional) Specifies a group to which this community belongs.
<i>group-name</i>	Name that identifies an existing group.
<b>ro</b>	(Optional) Specifies read-only access for this community.
<b>rw</b>	(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)SP1(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 named public:

```
n1010# configure terminal
n1010(config)# snmp-server community public ro
```

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

```
n1010# configure terminal
n1010(config)# no snmp-server community public
```

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

# 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]
```

<b>Syntax Description</b>	<i>name</i> (Optional) SNMP contact name (sysContact), which can contain a maximum of 32 characters.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	network-admin
---------------------------	---------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(4)SP1(1)	This command was introduced.

<b>Usage Guidelines</b>	You can create SNMP communities for SNMPv1 or SNMPv2c.
-------------------------	--

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

```
n1010# configure terminal
n1010(config)# snmp-server contact Admin
```

This example shows how to remove the sysContact:

```
n1010# configure terminal
n1010(config)# no snmp-server contact
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server aaa-user cache-timeout</b>	Configures how long the AAA-synchronized user configuration stays in the local cache.
	<b>snmp-server globalEnforcePriv</b>	Enforces SNMP message encryption for all users.
	<b>snmp-server host</b>	Configures a host receiver for SNMP traps or informs.

<b>Command</b>	<b>Description</b>
<b>snmp-server location</b>	Configures the sysLocation (the SNMP location).
<b>snmp-server protocol enable</b>	Enables SNMP.
<b>snmp-server tcp-session</b>	Enables a one-time authentication for SNMP over a TCP session.
<b>snmp-server user</b>	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)SP1(1)	This command was introduced.

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

```
n1010# configure terminal
n1010(config)# snmp-server globalEnforcePriv
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server aaa-user cache-timeout</b>	Configures how long the AAA-synchronized user configuration stays in the local cache.
	<b>snmp-server contact</b>	Configures sysContact (the SNMP contact).
	<b>snmp-server host</b>	Configures a host receiver for SNMP traps or informs.
	<b>snmp-server location</b>	Configures the sysLocation (the SNMP location).
	<b>snmp-server protocol enable</b>	Enables SNMP.
	<b>snmp-server tcp-session</b>	Enables a one-time authentication for SNMP over a TCP session.
	<b>snmp-server user</b>	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 {informs | traps} {version {1 | 2c | 3}} [auth | noauth | priv]
community [udp_port number]
```

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

Syntax Description		
<i>ip-address</i>		IPv4 address, IPv6 address, or Domain Name Service (DNS) name of the SNMP notification host.
<b>informs</b>		Specifies Inform messages to this host.
<b>traps</b>		Specifies Traps messages to this host.
<b>version</b>		Specifies the SNMP version to use for notification messages.
<b>1</b>		Specifies SNMPv1 as the version.
<b>2c</b>		Specifies SNMPv2c as the version.
<b>3</b>		Specifies SNMPv3 as the version.
<b>auth</b>	(Optional)	Specifies (for SNMPv3) the authNoPriv Security Level.
<b>noauth</b>	(Optional)	Specifies (for SNMPv3) the noAuthNoPriv Security Level.
<b>priv</b>	(Optional)	Specifies (for SNMPv3) the authPriv Security Level.
<i>community</i>		SNMPv1/v2c community string or SNMPv3 user name. The community string can be any alphanumeric string up to 255 characters.
<b>udp-port</b>	(Optional)	Specifies an existing UDP port.
<i>number</i>		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:

```
n1010# configure terminal
n1010(config)# snmp-server host 192.0.2.1 traps version 1 public
```

This example shows how to remove the configuration:

```
n1010# configure terminal
n1010(config)# no snmp-server host 192.0.2.1 traps version 1 public
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server aaa-user cache-timeout</b>	Configures how long the AAA-synchronized user configuration stays in the local cache.
	<b>snmp-server contact</b>	Configures the sysContact (the SNMP contact).
	<b>snmp-server globalEnforcePriv</b>	Enforces SNMP message encryption for all users.
	<b>snmp-server location</b>	Configures the sysLocation (the SNMP location).
	<b>snmp-server protocol enable</b>	Enables SNMP.
	<b>snmp-server tcp-session</b>	Enables a one-time authentication for SNMP over a TCP session.
	<b>snmp-server user</b>	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]
```

<b>Syntax Description</b>	<i>name</i> (Optional) SNMP location name (sysLocation), which can contain a maximum of 32 characters.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	network-admin
---------------------------	---------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(4)SP1(1)	This command was introduced.

**Examples** This example shows how to configure the sysLocation to be Lab-7:

```
n1010# configure terminal
n1010(config)# snmp-server location Lab-7
```

This example shows how to remove the sysLocation:

```
n1010# configure terminal
n1010(config)# no snmp-server location
```

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

Command	Description
<b>snmp-server protocol enable</b>	Enables SNMP.
<b>snmp-server tcp-session</b>	Enables a one-time authentication for SNMP over a TCP session.
<b>snmp-server user</b>	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)SP1(1)	This command was introduced.

**Examples** This example shows how to enable SNMP protocol operations:

```
n1010# configure terminal
n1010(config)# snmp-server protocol enable
```

This example shows how to disable SNMP protocol operations:

```
n1010# configure terminal
n1010(config)# no snmp-server protocol enable
```

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

Command	Description
<b>snmp-server tcp-session</b>	Enables a one-time authentication for SNMP over a TCP session.
<b>snmp-server user</b>	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)SP1(1)	This command was introduced.

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

```
n1010# configure terminal
n1010(config)# snmp-server tcp-session auth
```

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

```
n1010# configure terminal
n1010(config)# no snmp-server tcp-session
```

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

<i>name</i>	Name of a user who can access the SNMP engine.
<b>auth</b>	(Optional) Enables one-time authentication for SNMP over a TCP session
<b>md5</b>	(Optional) Specifies HMAC MD5 algorithm for authentication.
<b>sha</b>	(Optional) Specifies HMAC SHA algorithm for authentication.
<i>passphrase-1</i>	Authentication passphrase for this user. The passphrase can be any case-sensitive alphanumeric string up to 64 characters.
<b>priv</b>	(Optional) Specifies encryption parameters for the user.
<b>aes-128</b>	(Optional) Specifies a 128-byte AES algorithm for privacy.
<i>passphrase-2</i>	Encryption passphrase for this user. The passphrase can be any case-sensitive alphanumeric string up to 64 characters.
<b>engineID</b>	(Optional) Specifies the engineID for configuring the notification target user (for V3 informs).
<i>id</i>	Number that identifies the engineID, in a 12-digit, colon-separated decimal format.
<b>localizedkey</b>	(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)SP1(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:

```
n1010# configure terminal
n1010(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

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

```
n1010# configure terminal
n1010(config)# no snmp-server user Admin
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server aaa-user cache-timeout</b>	Configures how long the AAA-synchronized user configuration stays in the local cache.
	<b>snmp-server contact</b>	Configures the sysContact (the SNMP contact).
	<b>snmp-server globalEnforcePriv</b>	Enforces SNMP message encryption for all users.
	<b>snmp-server host</b>	Configures a host receiver for SNMP traps or informs.
	<b>snmp-server location</b>	Configures the sysLocation (the SNMP location).
	<b>snmp-server protocol enable</b>	Enables SNMP.
	<b>snmp-server tcp-session</b>	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)SP1(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:

```
n1010# configure terminal
n1010(config)# interface veth 2
n1010(config-if)# snmp trap link-status
n1010(config-if)#
```

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

```
n1010# configure terminal
n1010(config)# interface veth 2
n1010(config-if)# no snmp trap link-status
n1010(config-if)#
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server aaa-user cache-timeout</b>	Configures how long the AAA-synchronized user configuration stays in the local cache.
	<b>snmp-server contact</b>	Configures sysContact (the SNMP contact).

Command	Description
<b>snmp-server globalEnforcePriv</b>	Enforces SNMP message encryption for all users.
<b>snmp-server host</b>	Configures a host receiver for SNMP traps or informs.
<b>snmp-server location</b>	Configures the sysLocation (the SNMP location).
<b>snmp-server protocol enable</b>	Enables SNMP.
<b>snmp-server tcp-session</b>	Enables a one-time authentication for SNMP over a TCP session.

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

**Defaults** None

**Command Modes** Interface configuration (config-if)

**Supported User Roles** network-admin

Command History	Release	Modification
	4.0(4)SP1(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:

```
n1010 configure terminal
n1010(config)# interface ethernet 2/1
n1010(config-if)# speed 1000
```

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

```
n1010 configure terminal
n1010(config)# interface ethernet 2/1
n1010(config-if)# no speed 1000 11:00 AM
speed only present under mgmt0
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>duplex</b>	Specifies the duplex mode as full, half, or autonegotiate.
<b>interface</b>	Specifies the interface that you are configuring.
<b>show interface</b>	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	
<i>username</i>	(Optional) Username for the SSH session. The username is not case sensitive.
<i>ipv4-address</i>	IPv4 address of the remote device.
<i>hostname</i>	Hostname of the remote device. The hostname is case sensitive.
<b>vrf</b> <i>vrf-name</i>	(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 command mode

**SupportedUserRoles** network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

**Usage Guidelines** The Cisco NX-OS software supports SSH version 2.

**Examples** This example shows how to start an SSH session:

```
n1010# 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
	<b>clear ssh session</b>	Clears SSH sessions.
	<b>ssh server enable</b>	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

<b>dsa</b>	Specifies the Digital System Algorithm (DSA) SSH server key.
<b>force</b>	(Optional) Forces the replacement of an SSH key.
<b>rsa</b>	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
<i>length</i>	(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)

## Supported User Roles

network-admin

## Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

## Usage Guidelines

The switch uses a 1024-bit RSA key by default. The **ssh key** command allows you to choose a different algorithm (DSA) or different key strengths.

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.

The Cisco NX-OS software supports SSH version 2.

## Examples

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

```
n1010# configure terminal
n1010(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:

```
n1010# configure terminal
```

```
n1010(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:

```
n1010# configure terminal
n1010(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:

```
n1010# configure terminal
n1010(config)# no ssh server enable
n1010(config)# ssh key dsa force
deleting old dsa key.....
generating dsa key(1024 bits).....
.
generated dsa key
n1010(config)# ssh server enable
```

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

```
n1010# configure terminal
n1010(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
n1010(config)# no ssh key dsa
n1010(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

```
n1010# configure terminal
n1010(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
n1010(config)# no ssh key
n1010(config)# ssh server enable
```

#### Related Commands

Command	Description
<b>show ssh key</b>	Displays the SSH server key information.
<b>ssh server enable</b>	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)SP1(1)	This command was introduced.

**Usage Guidelines** The Cisco NX-OS software supports SSH version 2.

**Examples** This example shows how to enable the SSH server:

```
n1010# configure terminal
n1010(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
n1010# configure terminal
n1010(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
```

Related Commands	Command	Description
	<b>show ssh server</b>	Displays the SSH server key 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)SP1(1)	This command was introduced.

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

```
n1010# configure terminal
n1010(config)# svs-domain
n1010(config-svs-domain)#
```

Related Commands	Command	Description
	<b>show svs</b>	Displays SVS information.

# 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**

<b>Syntax Description</b>	<i>name</i>	Name for the device. The name is alphanumeric, case sensitive, can contain special characters, and can have a maximum of 32 characters.
---------------------------	-------------	---

<b>Defaults</b>	switch
-----------------	--------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>SupportedUserRoles</b>	network-admin
---------------------------	---------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(4)SP1(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:

```
n1010# configure terminal
n1010(config)# switchname Engineering2
Engineering2(config)#
```

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

```
Engineering2# configure terminal
Engineering2(config)# no switchname
n1010(config)#
```

# 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		
	<b>primary</b>	Specifies the primary redundant VSM.
	<b>secondary</b>	Specifies the secondary redundant VSM.
	<b>standalone</b>	Specifies no redundant VSM.

Command Default	
	None

Command Modes	
	EXEC

SupportedUserRoles	
	network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

**Examples** This example shows how to configure no redundant VSM:

```
n1010# system redundancy role standalone
n1010#
```

Related Commands	Command	Description
	<b>reload module</b>	Reloads the Virtual Supervisor Module (VSM).
	<b>show version</b>	Displays the software version is present on the VSM.

# 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)SP1(1)	This command was introduced.

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

```
n1010# system switchover
n1010#
```

Related Commands	Command	Description
	<b>reload module</b>	Reloads the Virtual Supervisor Module (VSM).
	<b>show version</b>	Displays the software version is present on the VSM.
	<b>system redundancyrole</b>	Configures a redundancy role for the VSM.