CHAPTER 6

Configuring SSH and Telnet

This chapter describes how to configure Secure Shell Protocol (SSH) and Telnet on Cisco NX-OS devices.

This chapter includes the following sections:

Information About SSH and Telnet

This section includes the following topics:

SSH Server

You can use the SSH server to enable an SSH client to make a secure, encrypted connection to a Cisco NX-OS device. SSH uses strong encryption for authentication. The SSH server in the Cisco NX-OS software can interoperate with publicly and commercially available SSH clients.

The user authentication mechanisms supported for SSH are RADIUS, TACACS+, and the use of locally stored usernames and passwords.

SSH Client

The SSH client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco NX-OS device to make a secure, encrypted connection to another Cisco NX-OS device or to any other device that runs the SSH server. This connection provides an outbound connection that is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco NX-OS software works with publicly and commercially available SSH servers.

SSH Server Keys

SSH requires server keys for secure communications to the Cisco NX-OS device. You can use SSH server keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSH version 2 using the Digital System Algrorithm (DSA)

Be sure to have an SSH server key-pair with the appropriate version before enabling the SSH service. You can generate the SSH server key-pair according to the SSH client version used. The SSH service accepts two types of key-pairs for use by SSH version 2:

- The **dsa** option generates the DSA key-pair for the SSH version 2 protocol.
- The **rsa** option generates the RSA key-pair for the SSH version 2 protocol.

By default, the Cisco NX-OS software generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)

Caution If you delete all of the SSH keys, you cannot start the SSH services.

SSH Authentication Using Digital Certificates

SSH authentication on NX-OS devices provides X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that ensures the origin and integrity of a message. It contains encryption keys for secured communications and is “signed” by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through query or notification. Verification of certificates is successful if the certificates are from any of the trusted CAs.

You can configure your device for either SSH authentication using an X.509 certificate or SSH authentication using a Public Key Certificate, but not both. If either of them is configured and the authentication fails, you are prompted for a password.

For more information on CAs and digital certificates, see Chapter 5, "Configuring PKI."

Telnet Server

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

The Telnet server is disabled by default on the NX-OS device.

Virtualization Support

SSH and Telnet configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1*.

Licensing Requirements for SSH and Telnet

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	SSH and Telnet require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*.

Prerequisites for SSH

SSH and Telnet have the following prerequisites:

- You have configured IP on a Layer 3 interface, out-of-band on the mgmt 0 interface, or inband on an Ethernet interface.

Guidelines and Limitations

SSH and Telnet have the following configuration guidelines and limitations:

- The Cisco NX-OS software supports only SSH version 2 (SSHv2).
- You can configure your device for either SSH authentication using an X.509 certificate or SSH authentication using a Public Key Certificate, but not both. If either of them is configured and the authentication fails, you are prompted for a password.
- The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring SSH

This section includes the following sections:

Generating SSH Server Keys

You can generate an SSH server key based on your security requirements. The default SSH server key is an RSA key that is generated using 1024 bits.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **no feature ssh**
3. **ssh key** {**dsa** [**force**] | **rsa** [*bits* **[force**]]}
4. **feature ssh**
5. **exit**
6. **show ssh key**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**no feature ssh** **Example:** switch(config)# no feature ssh	Disables SSH.
Step 3	**ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]} **Example:** switch(config)# ssh key rsa 2048	Generates the SSH server key. The *bits* argument is the number of bits used to generate the key. The range is from 768 to 2048 and the default value is 1024. Use the **force** keyword to replace an existing key.
Step 4	**feature ssh** **Example:** switch(config)# feature ssh	Enables SSH.
Step 5	**exit** **Example:** switch(config)# exit switch#	Exits global configuration mode.
Step 6	**show ssh key** **Example:** switch# show ssh key	(Optional) Displays the SSH server keys.
Step 7	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Specifying the SSH Public Keys for User Accounts

You can configure an SSH public key to log in using an SSH client without being prompted for a password. You can specify the SSH public key in one of these formats:

- OpenSSH format
- IETF SECSH format

Specifying the SSH Public Keys in OpenSSH Format

You can specify the SSH public keys in OpenSSH format for user accounts.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Generate an SSH public key in OpenSSH format.

SUMMARY STEPS

1. **config t**
2. **username** *username* **sshkey** *ssh-key*
3. **exit**
4. **show user-account**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**username** *username* **sshkey** *ssh-key* **Example:** switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1X swK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/ DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG 30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH 3UD/vKyziEh5S4Tplx8=	Configures the SSH public key in OpenSSH format.
Step 3	**exit** **Example:** switch(config)# exit switch#	Exits global configuration mode.
Step 4	**show user-account** **Example:** switch# show user-account	(Optional) Displays the user account configuration.
Step 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Specifying the SSH Public Keys in IETF SECSH Format

You can specify the SSH public keys in IETF SECSH format for user accounts.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

You have generated an SSH public key in IETF SCHSH format.

SUMMARY STEPS

1. **copy** *server-file* **bootflash:***filename*

2. **config t**
3. **username** *username* **sshkey file bootflash:***filename*
4. **exit**
5. **show user-account**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**copy** *server-file* **bootflash:***filename* **Example:** `switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub`	Downloads the file containing the SSH key in IETF SECSH format from a server. The server can be FTP, secure copy (SCP), secure FTP (SFTP), or TFTP.

Step 2	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**username** *username* **sshkey file bootflash:***filename* **Example:** `switch(config)# username User1 sshkey file bootflash:secsh_file.pub`	Configures the SSH public key in IETF SECSH format.

Step 4	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	**show user-account** **Example:** `switch# show user-account`	(Optional) Displays the user account configuration.
Step 6	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Starting SSH Sessions

You can start SSH sessions using IPv4 or IPv6 to connect to remote devices from the Cisco NX-OS device.

Note The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

BEFORE YOU BEGIN

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSH server on the remote device.

SUMMARY STEPS

1. **ssh** [*username*@]{*hostname* | *username*@*hostname*} [**vrf** *vrf-name*]
   ssh6 [*username*@]{*hostname* | *username*@*hostname*} [**vrf** *vrf-name*]

DETAILED STEPS

	Command	Purpose
Step 1	**ssh** [*username*@]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*] **Example:** switch# ssh 10.10.1.1	Creates an SSH IPv4 session to a remote device using IPv4. The default VRF is the default VRF.
	ssh6 [*username*@]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*] **Example:** switch# ssh6 HostA	Creates an SSH IPv6 session to a remote device using IPv6.

Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, or when you start an SSH session from this device to a remote host, you establish a trusted SSH relationship with that server. You can clear the list of trusted SSH servers for your user account.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **clear ssh hosts**

DETAILED STEPS

	Command	Purpose
Step 1	**clear ssh hosts** **Example:** switch# clear ssh hosts	Clears the SSH host sessions.

Disabling the SSH Server

By default, the SSH server is enabled on the NX-OS device. You can disable the SSH server to prevent SSH access to the switch.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. config t
2. no feature ssh
3. exit
4. show ssh server
5. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**no feature ssh** **Example:** switch(config)# no feature ssh	Disables the SSH server. The default is enabled.
Step 3	**exit** **Example:** switch(config)# exit switch#	Exits global configuration mode.
Step 4	**show ssh server** **Example:** switch# show ssh server	(Optional) Displays the SSH server configuration.
Step 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Deleting SSH Server Keys

You can delete SSH server keys after you disable the SSH server.

Note To reenable SSH, you must first generate an SSH server key (see the "Generating SSH Server Keys" section on page 6-4).

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. config t
2. no feature ssh

3. **no ssh key** [**dsa** | **rsa**]
4. **exit**
5. **show ssh key**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**no feature ssh** **Example:** switch(config)# no feature ssh	Disables the SSH server.
Step 3	**no ssh key** [**dsa** | **rsa**] **Example:** switch(config)# no ssh key rsa	Deletes the SSH server key. The default is to delete all the SSH keys.
Step 4	**exit** **Example:** switch(config)# exit switch#	Exits global configuration mode.
Step 5	**show ssh key** **Example:** switch# show ssh key	(Optional) Displays the SSH server key configuration.
Step 6	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Clearing SSH Sessions

You can clear SSH sessions from the Cisco NX-OS device.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **show users**
1. **clear line** *vty-line*

DETAILED STEPS

	Command	Purpose
Step 1	**show users** **Example:** switch# show users	Displays user session information.
Step 2	**clear line** *vty-line* **Example:** switch(config)# clear line pts/12	Clears a user SSH session.

Configuring Telnet

This section includes the following topics:

Enabling the Telnet Server

You can enable the Telnet server on the Cisco NX-OS device. By default, the Telnet server is disabled.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **feature telnet**
3. **exit**
4. **show telnet server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**feature telnet** **Example:** switch(config)# feature telnet	Enables the Telnet server. The default is disabled.
Step 3	**exit** **Example:** switch(config)# exit switch#	Exits global configuration mode.
Step 4	**show telnet server** **Example:** switch# show telnet server	(Optional) Displays the Telnet server configuration.
Step 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Starting Telnet Sessions to Remote Devices

You can start Telnet sessions to connect to remote devices from the Cisco NX-OS device. You can start Telnet sessions using either IPv4 or , in Cisco NX-OS Release 4.0(2) and later releases, IPv6.

Note The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

BEFORE YOU BEGIN

Obtain the hostname or IP address for the remote device and, if needed, the username on the remote device.

Enable the Telnet server on the NX-OS device (see the "Enabling the Telnet Server" section on page 6-11).

Enable the Telnet server on the remote device.

SUMMARY STEPS

1. **telnet** {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]
   telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

DETAILED STEPS

	Command	Purpose
Step 1	**telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*] **Example:** switch# telnet 10.10.1.1	Starts a Telnet session to a remote device using IPv4. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF.
	telnet6 {*ipv6-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*] **Example:** switch# telnet 2001:0DB8::ABCD:1 vrf management	Starts a Telnet session to a remote device using IPv6. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF. **Note** Cisco NX-OS Release 4.0(2) and later releases suport IPv6 for starting Telnet session.

Clearing Telnet Sessions

You can clear Telnet sessions from the Cisco NX-OS device.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Enable the Telnet server on the NX-OS device.

SUMMARY STEPS

1. **show users**
2. **clear line** *vty-line*

DETAILED STEPS

	Command	Purpose
Step 1	**show users** **Example:** switch# show users	Displays user session information.
Step 2	**clear line** *vty-line* **Example:** switch(config)# clear line pts/12	Clears a user Telnet session.

Verifying the SSH and Telnet Configuration

To display the SSH and Telnet configuration information, perform one of the following tasks:

Command	Purpose
show ssh key [dsa | rsa]	Displays SSH server key-pair information.
show running-config security [**all**]	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh server	Displays the SSH server configuration.
show telnet server	Displays the SSH server configuration.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*.

SSH Example Configuration

To configure SSH with an OpenSSH key, follow these steps:

Step 1 Disable the SSH server.

```
switch# config t
switch(config)# no feature ssh
```

Step 2 Generate an SSH server key.

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

Step 3 Enable the SSH server.

```
switch(config)# feature ssh
```

Step 4 Display the SSH server key.

```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
************************************
could not retrieve dsa key information
************************************
```

Step 5 Specify the SSH public key in OpenSSH format.

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZ19G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
```

Step 6 Save the configuration.

```
switch(config)# copy running-config startup-config
```

Default Settings

Table 6-1 lists the default settings for SSH and Telnet parameters.

Table 6-1 Default SSH and Telnet Parameters

Parameters	Default
SSH server	Enabled.
SSH server key	RSA key generated with 1024 bits.
RSA key bits for generation	1024.
Telnet server	Disabled.
Telnet port number	23.

Additional References

For additional information related to implementing RBAC, see the following sections:

- Related Documents, page 6-15
- Standards, page 6-16
- MIBs, page 6-16

Related Documents

Related Topic	Document Title
Licensing	*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.1*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-SECURE-SHELL-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for SSH and Telnet

Table 6-2 lists the release history for these features.

Table 6-2 Feature History for SSH and Telnet

Feature Name	Releases	Feature Information
Digital certificate support	4.1(2)	Added support for digital certificates.
Enabling SSH server	4.1(2)	Added the **feature ssh** command and deprecated the **ssh server enable** command.
Enabling Telnet server	4.1(2)	Added the **feature telnet** command and deprecated the **telnet server enable** command.
IPv6 support	4.0(2)	Added the **telnet6** command.
SSH and Telnet	4.0(1)	This feature was introduced.