CHAPTER 1

Configuring SSH and Telnet

This chapter describes how to configure Secure Shell Protocol (SSH) and Telnet on the Nexus 5000 Series switches.

This chapter includes the following sections:

Information About SSH and Telnet

This section includes the following topics:

SSH Server

The SSH server feature enables a SSH client to make a secure, encrypted connection to a Nexus 5000 Series switch. SSH uses strong encryption for authentication. The SSH server in the Nexus 5000 Series switch will interoperate with publicly and commercially available SSH clients.

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

SSH Client

The SSH client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a Nexus 5000 Series switch to make a secure, encrypted connection to another Nexus 5000 Series switch or to any other device running 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 Nexus 5000 Series switch works with publicly and commercially available SSH servers.

SSH Server Keys

SSH requires server keys for secure communications to the Nexus 5000 Series switch. You can use SSH 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 three 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 Nexus 5000 Series switch generates an RSA key using 1024 bits.

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

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 system to the other. Telnet can accept either an IP address or a domain name as the remote system address.

The Telnet server is enabled by default on the Nexus 5000 Series switch.

Prerequisites for SSH

SSH 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 have the following configuration guidelines and limitations:

- The Nexus 5000 Series switch supports only SSH version 2 (SSHv2).

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, page 1-3
- Specifying the SSH Public Keys for User Accounts, page 1-4
- Starting SSH Sessions to Remote Devices, page 1-6
- Clearing SSH Hosts, page 1-6
- Disabling the SSH Server, page 1-6
- Deleting SSH Server Keys, page 1-7
- Clearing SSH Sessions, page 1-7

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 generated using 1024 bits. To generate SSH server keys, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# ssh key {dsa [force] | rsa [bits [force]]}`	Generates the SSH server key. The *bits* argument is the number of bits used to generate the key. The range is 768 to 2048 and the default value is 1024. Use the **force** keyword to replace an existing key.
Step 3	`switch(config)# exit`	Exits global configuration mode.
Step 4	`switch# show ssh key`	(Optional) Displays the SSH server keys.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to generate an SSH server key:

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

Specifying the SSH Public Keys for User Accounts

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

- Open SSH format
- IETF SECSH format
- Public Key Certificate in PEM format

Specifying the SSH Public Keys in Open SSH Format

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

To specify the SSH public keys in open SSH format, generate an SSH public key in open SSH format and perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **username** *username* **sshkey** *ssh-key*	Configures the SSH public key in SSH format.
Step 3	switch(config)# **exit**	Exits global configuration mode.
Step 4	switch# **show user-account**	(Optional) Displays the user account configuration.
Step 5	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to specify an SSH public keys in open SSH format:

```
switch# configure terminal
switch(config)# switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

Specifying the SSH Public Keys in IETF SECSH Format

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

To specify the SSH public keys in IETF SECSH format, generate an SSH public key in IETF SCHSH format, and perform this task:

	Command	Purpose
Step 1	`switch# copy server-file bootflash:filename`	Downloads the file containing the SSH key in IETF SECSH format from a server. The server can be FTP, SCP, SFTP, or TFTP.
Step 2	`switch# configure terminal`	Enters configuration mode.
Step 3	`switch(config)# username username sshkey file filename`	Configures the SSH public key in SSH format.
Step 4	`switch(config)# exit`	Exits global configuration mode.
Step 5	`switch# show user-account`	(Optional) Displays the user account configuration.
Step 6	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to specify the SSH public keys in the IETF SECSH format:

```
switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

Specifying the SSH Public Keys in PEM-Formatted Public Key Certificate Form

You can specify the SSH public keys in PEM-formatted Public Key Certificate form for user accounts.

To specify the SSH public keys in PEM-formatted Public Key Certificate form, generate an SSH public key in PEM-Formatted Public Key Certificate form and perform this task:

	Command	Purpose
Step 1	`switch# copy server-file bootflash:filename`	Downloads the file containing the SSH key in PEM-formatted Public Key Certificate form from a server. The server can be FTP, SCP, SFTP, or TFTP
Step 2	`switch# configure terminal`	Enters configuration mode.
Step 3	`switch# show user-account`	(Optional) Displays the user account configuration.
Step 4	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to specify the SSH public keys in PEM-formatted public key certificate form:

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

Starting SSH Sessions to Remote Devices

You can start SSH sessions to connect to remote devices from your Nexus 5000 Series switch.

	Command	Purpose
Step 1	`switch# ssh {hostname	username@hostname} [vrf vrf-name]`	Creates an SSH session to a remote device. The *hostname* argument can be an IPv4 address, an IPv6 address, or a device name.

Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, you establish a trusted SSH relationship with that server. To clear the list of trusted SSH servers for your user account, perform this task:

	Command	Purpose
Step 1	`switch# clear ssh hosts`	Clears the SSH host sessions.

Disabling the SSH Server

By default, the SSH server is enabled on the Nexus 5000 Series switch.

To disable the SSH server to prevent SSH access to the switch, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# [no] feature ssh`	Enables/disables the SSH server. The default is enabled.
Step 3	`switch(config)# exit`	Exits global configuration mode.
Step 4	`switch# show ssh server`	(Optional) Displays the SSH server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Send feedback to nx5000-docfeedback@cisco.com

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 "Generating SSH Server Keys" section on page 1-3).

To delete the SSH server keys, perform this task:

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

Clearing SSH Sessions

To clear SSH sessions from the Nexus 5000 Series switch, perform this task:

	Command	Purpose
Step 1	`switch# show users`	Displays user session information.
Step 2	`switch(config)# clear line vty-line`	Clears a user SSH session.

Configuring Telnet

This section includes the following topics:

- Clearing SSH Sessions, page 1-7
- Starting Telnet Sessions to Remote Devices, page 1-8
- Clearing SSH Sessions, page 1-7

Enabling the Telnet Server

By default, the Telnet server is enabled. To disable the Telnet server on your Nexus 5000 Series switch, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# [no] feature telnet`	Enables/disables the Telnet server. The default is enabled.

To reenable the Telnet server, perform this task:

Command	Purpose
`switch(config)# telnet server enable`	Reenables the Telnet server.

Starting Telnet Sessions to Remote Devices

Before you start a Telnet session to connect to remote devices, you should do the following:

- Obtain the hostname for the remote device and, if needed, the user name on the remote device.
- Enable the Telnet server on the Nexus 5000 Series switch.
- Enable the Telnet server on the remote device.

To start Telnet sessions to connect to remote devices from your Nexus 5000 Series switch, perform this task:

	Command	Purpose
Step 1	`switch# telnet hostname`	Creates a Telnet session to a remote device. The *hostname* argument can be an IPv4 address, an IPv6 address, or a device name.

The following example shows starting a Telnet session to connect to a remote device:

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

Clearing Telnet Sessions

To clear Telnet sessions from the Nexus 5000 Series switch, perform this task:

	Command	Purpose
Step 1	`switch# show users`	Displays user session information.
Step 2	`switch(config)# clear line vty-line`	Clears a user Telnet session.

Send feedback to nx5000-docfeedback@cisco.com

Verifying the SSH and Telnet Configuration

To display the SSH 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 user-account	Displays user account information.

SSH Example Configuration

The following example shows how to configure SSH:

Step 1 Generate an SSH server key.

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

Step 2 Enable the SSH server.

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

Step 3 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 4 Specify the SSH public key in Open SSH format.

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
```

Step 5 Save the configuration.

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

Send feedback to nx5000-docfeedback@cisco.com

Default Settings

Table 1-1 lists the default settings for SSH parameters.

Table 1-1 Default SSH Parameters

Parameters	Default
SSH server	Enabled
SSH server key	RSA key generated with 1024 bits
RSA key bits for generation	1024
Telnet server	Enabled