CHAPTER 4

Configuring TACACS+

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on Cisco NX-OS devices.

This chapter includes the following sections:

Information About TACACS+

The TACACS+ security protocol provides centralized validation of users attempting to gain access to a Cisco NX-OS device. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your NX-OS device are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The TACACS+ client/server protocol uses TCP (TCP port 49) for transport requirements. Cisco NX-OS devices provide centralized authentication using the TACACS+ protocol.

This section includes the following topics:

- TACACS+ Advantages, page 4-2
- TACACS+ Operation for User Login, page 4-2
- Default TACACS+ Server Encryption Type and Secret Key, page 4-3
- TACACS+ Server Monitoring, page 4-3
- TACACS+ Configuration Distribution, page 4-4
- Vendor-Specific Attributes, page 4-5
- Virtualization Support, page 4-6

TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Cisco NX-OS device can authorize access without authenticating.
- Uses the TCP transport protocol to send data between the AAA client and server, making reliable transfers with a connection-oriented protocol.
- Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only encrypts passwords.

TACACS+ Operation for User Login

When a user attempts a Password Authentication Protocol (PAP) login to a Cisco NX-OS device using TACACS+, the following actions occur:

1. When the Cisco NX-OS device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.

Note TACACS+ allows an arbitrary conversation between the daemon and the user until the daemon receives enough information to authenticate the user. This action is usually done by prompting for a username and password combination, but may include prompts for other items, such as mother's maiden name.

2. The Cisco NX-OS device will eventually receive one of the following responses from the TACACS+ daemon:

   a. ACCEPT—User authentication succeeds and service begins. If the Cisco NX-OS device requires user authorization, authorization begins.

   b. REJECT—User authentication failed. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.

   c. ERROR—An error occurred at some time during authentication either at the daemon or in the network connection between the daemon and the Cisco NX-OS device. If the Cisco NX-OS device receives an ERROR response, the Cisco NX-OS device tries to use an alternative method for authenticating the user.

After authentication, the user also undergoes an additional authorization phase if authorization has been enabled on the Cisco NX-OS device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the Cisco NX-OS device again contacts the TACACS+ daemon and it returns an ACCEPT or REJECT authorization response. An ACCEPT response contains attributes that are used to direct the EXEC or NETWORK session for that user and determines the services that the user can access.

   Services include the following:

   - Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
   - Connection parameters, including the host or client IP address (IPv4 or IPv6), access list, and user timeouts

Default TACACS+ Server Encryption Type and Secret Key

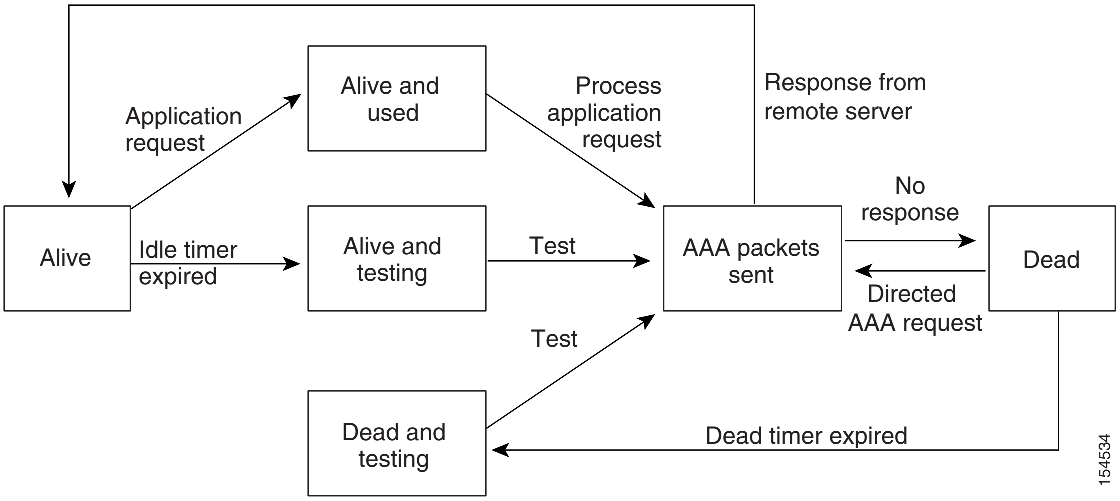
You must configure the TACACS+ secret key to authenticate the switch to the TACACS+ server. A secret key is a secret text string shared between the Cisco NX-OS device and the TACACS+ server host. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global secret key for all TACACS+ server configurations on the Cisco NX-OS device to use.

You can override the global secret key assignment by explicitly using the **key** option when configuring and individual TACACS+ server.

TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco NX-OS device can periodically monitor an TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco NX-OS device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. A Cisco NX-OS device periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. This process verifies that a TACACS+ server is in a working state before real AAA requests are sent its way. Whenever an TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco NX-OS device displays an error message that a failure is taking place before it can impact performance. See Figure 4-1.

Figure 4-1 TACACS+ Server States



Note The monitoring interval for alive servers and dead servers are different and can be configured by the user. The TACACS+ server monitoring is performed by sending a test authentication request to the TACACS+ server.

TACACS+ Configuration Distribution

Cisco Fabric Services (CFS) allows the Cisco NX-OS device distribute the TACACS+ configuration to other NX-OS devices in the network. When you enable CFS distribution for a feature on your device, the device belongs to a CFS region containing other devices in the network that you have also enabled for CFS distribution for the feature. CFS distribution for TACACS+ is disabled by default.

Note You must explicitly enable CFS for TACACS+ on each device to which you want to distribute configuration changes.

After you enable CFS distribution for TACACS+ on your NX-OS device, the first TACACS+ configuration command that you enter causes the Cisco NX-OS software to take the following actions:

- Creates a CFS session on your NX-OS device.
- Locks the TACACS+ configuration on all NX-OS devices in the CFS region with CFS enabled for TACACS+.
- Saves the TACACS+ configuration changes in a temporary buffer on the Cisco NX-OS device.

The changes stay in the temporary buffer on the Cisco NX-OS device until you explicitly commit them to be distributed to the devices in the CFS region. When you commit the changes, the Cisco NX-OS software takes the following actions:

- Applies the changes to the running configuration on your NX-OS device.
- Distributes the updated TACACS+ configuration to the other NX-OS devices in the CFS region.
- Unlocks the TACACS+ configuration in the devices in the CFS region.
- Terminates the CFS session.

CFS does not distribute the TACACS+ server group configurations, periodic TACACS+ server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other NX-OS devices.

For detailed information on CFS, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.1*.

Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the TACACS+ server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

This section includes the following topics:

- Cisco VSA Format, page 4-5
- Cisco TACACS+ Privilege Levels, page 4-6

Cisco VSA Format

The Cisco TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use TACACS+ servers for authentication on a Cisco NX-OS device, the TACACS+ protocol directs the TACACS+ server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Cisco NX-OS software:

- Shell—Protocol used in access-accept packets to provide user profile information.
- Accounting—Protocol used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Cisco NX-OS software supports the following attributes:

- roles—Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white space. For example, if the user belongs to roles network-operator and vdc-admin, the value field would be “network-operator vdc-admin.” This subattribute, which the TACACS+ server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute as supported by Cisco ACS:

  ```
  shell:roles=“network-operator vdc-admin”

  shell:roles*“network-operator vdc-admin”
  ```

Note When you specify a VSA as shell:roles*“network-operator vdc-admin”, this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

- accountinginfo—Stores accounting information in addition to the attributes covered by a standard TACACS+ accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the TACACS+ client on the switch. It can be used only with the accounting protocol data units (PDUs).

Cisco TACACS+ Privilege Levels

TACACS+ servers support privilege levels for specifying the permissions that users have when logging into a Cisco NX-OS device. For the maximum privilege level 15, the Cisco NX-OS software applies the network-admin role in the default VDC or the vdc-admin role for nondefault VDCs. All other privilege levels are translated to the vdc-operator role. For more information on user roles, see Chapter 7, “Configuring User Accounts and RBAC.”

Note If you specify a user role in the cisco-av-pair, that takes precedence over the privilege level.

Virtualization Support

TACACS+ 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*.

The Cisco NX-OS device uses virtual routing and forwarding instances (VRFs) to access the TACACS+ servers. For more information on VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.1*.

Licensing Requirements for TACACS+

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	TACACS+ requires 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 Cisco NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*.

Prerequisites for TACACS+

TACACS+ has the following prerequisites:

- Obtain the IPv4 or IPv6 addresses or hostnames for the TACACS+ servers.
- Obtain the secret keys from the TACACS+ servers, if any.
- Ensure that the Cisco NX-OS device is configured as a TACACS+ client of the AAA servers.

Guidelines and Limitations

TACACS+ has the following guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers on the Cisco NX-OS device.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

Configuring TACACS+

This section includes the following topics:

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.

TACACS+ Server Configuration Process

To configure TACACS+ servers, follow these steps:

Step 1 Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

Step 2 If needed, enable CFS configuration distribution for TACACS+ (see the"Enabling TACACS+ Configuration Distribution" section on page 4-9).

Step 3 Establish the TACACS+ server connections to the Cisco NX-OS device (see the "Configuring TACACS+ Server Hosts" section on page 4-10).

Step 4 Configure the secret keys for the TACACS+ servers (see the "Configuring Global TACACS+ Keys" section on page 4-11 and the "Configuring a Key for a Specific TACACS+ Server" section on page 4-13).

Step 5 If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods (see the "Configuring TACACS+ Server Groups" section on page 4-14 and the "Configuring AAA" section on page 2-7).

Step 6 If needed, configure any of the following optional parameters:

- Dead-time interval (see the "Configuring the Dead-Time Interval" section on page 4-23).
- TACACS+ server specification allowed at user login (see the "Specifying a TACACS+ Server at Login" section on page 4-17).
- Timeout interval (see the "Configuring the Global TACACS+ Timeout Interval" section on page 4-18).
- TCP port (see the "Configuring TCP Ports" section on page 4-20).

Step 7 If needed, configure periodic TACACS+ server monitoring (see the "Configuring Periodic TACACS+ Server Monitoring" section on page 4-22).

Step 8 If TACACS+ distribution is enable, commit the TACACS+ configuration to the fabric (see the "Committing the TACACS+ Configuration to Distribution" section on page 4-26).

Enabling TACACS+

By default, the TACACS+ feature is disabled on the Cisco NX-OS device. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for authentication.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. **configure terminal**
2. **feature tacacs+**
3. **exit**
4. **show feature**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`feature tacacs+`**
	
	Example:
	`switch(config)# feature tacacs+`
		Enables TACACS+.

Step 3	**`exit`**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 4	**`show feature`**
	
	Example:
	`switch# show feature`
		(Optional) Displays the enabled status of the feature.

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

Enabling TACACS+ Configuration Distribution

Only NX-OS devices that have distribution enabled can participate in the distribution of the TACACS+ configuration changes in the CFS region.

BEFORE YOU BEGIN

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

Ensure that CFS distribution is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs+ distribute**
3. **exit**
4. **show tacacs+ status**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	
	`Example:`
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	`switch(config)#` **`tacacs+ distribute`**
	
	`Example:`
	`switch(config)# tacacs+ distribute`
		Enable TACACS+ configuration distribution. The default is disabled.

Step 3	**`exit`**
	
	`Example:`
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 4	**`show tacacs+ status`**
	
	`Example:`
	`switch(config)# show tacacs+ status`
		(Optional) Displays the TACACS+ CFS distribution configuration.

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

Configuring TACACS+ Server Hosts

To access a remote TACACS+ server, you must configure the IP address or the hostname for the TACACS+ server on the Cisco NX-OS device. You can configure up to 64 TACACS+ servers.

Note By default, when you configure a TACACS+ server IP address or hostname the Cisco NX-OS device, the TACACS+ server is added to the default TACACS+ server group. You can also add the TACACS+ server to another TACACS+ server group. For information about creating TACACS+ server groups, see the "Configuring TACACS+ Server Groups" section on page 4-14).

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

Obtain the IPv4 or IPv6 addresses or the hostnames for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
3. **show tacacs+** {**pending** | **pending-diff**}
4. **tacacs+ commit**

5. **exit**
6. **show tacacs-server**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
	
	Example:
	`switch(config)# tacacs-server host 10.10.2.2`
		Specifies the IPv4 or IPv6 address or hostname for a TACACS+ server.

Step 3	**show tacacs+** {**pending** | **pending-diff**}
	
	Example:
	`switch(config)# show tacacs+ distribution pending`
		(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

Step 4	**tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices in the network that you have enabled CFS configuration distribution for the TACACS+ feature.

Step 5	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	**show tacacs-server** **Example:** `switch# show tacacs-server`	(Optional) Displays the TACACS+ server configuration.
Step 7	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring Global TACACS+ Keys

You can configure secret TACACS+ keys at the global level for all servers used by the Cisco NX-OS device. A secret key is a shared secret text string between the Cisco NX-OS device and the TACACS+ server hosts.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

Obtain the secret key values for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server key** [**0** | **7**] *key-value*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`tacacs-server key`** `[`**`0`** `|` **`7`**`]` *`key-value`*
	Example:
	`switch(config)# tacacs-server key 0 QsEfThUkO`
		Specifies a TACACS+ key for all TACACS+ server. You can specify that the *key-value* is in clear text (**0**) format or is encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters.
		By default, no secret key is configured.

Step 3	**`exit`**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 4	**`show tacacs-server`**
	Example:
	`switch# show tacacs-server`
		(Optional) Displays the TACACS+ server configuration.
		Note The secret keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted secret keys.

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

Configuring a Key for a Specific TACACS+ Server

You can configure secret keys for a TACACS+ server. A secret key is a shared secret text string between the Cisco NX-OS device and the TACACS+ server host.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

Obtain the secret key values for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value*
3. **show tacacs+** {**pending** | **pending-diff**}
4. **tacacs+ commit**
5. **exit**
6. **show tacacs-server**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`tacacs-server host`** {*`ipv4-address`* | *`ipv6-address`* | *`host-name`*} **`key`** [**`0`** | **`7`**] *`key-value`*
	Example:
	`switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg`
		Specifies a secret key for a specific TACACS+ server. You can specify that the *key-value* is in clear text (**0**) format or is encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters.
		This secret key is used instead of the global secret key.

Step 3	**`show tacacs+`** {**`pending`** | **`pending-diff`**}
	Example:
	`switch(config)# show tacacs+ pending`
		(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

Step 4	**`tacacs+ commit`**
	Example:
	`switch(config)# tacacs+ commit`
		(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

	Command	Purpose

Step 5	`exit`
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	`show tacacs-server`
	Example:
	`switch# show tacacs-server`
		(Optional) Displays the TACACS+ server configuration.
		Note The secret keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted secret keys.

Step 7	`copy running-config startup-config`
	Example:
	`switch# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Configuring TACACS+ Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the TACACS+ protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service. For information on AAA services, see the "Remote AAA Services" section on page 2-3.

Note CFS does not distribute TACACS+ server group configurations.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server tacacs+** *group-name*
3. **server** {*ipv4-address* | *ipv6-address* | *host-name*}
4. **deadtime** *minutes*
5. **source-interface** *interface*
6. **use-vrf** *vrf-name*
7. **exit**
8. **show tacacs-server groups**
9. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`aaa group server tacacs+`** *`group-name`*
	Example:
	`switch(config)# aaa group server tacacs+ TacServer`
	`switch(config-tacacs+)#`
		Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.

Step 3	**`server`** {*`ipv4-address`* | *`ipv6-address`* | *`host-name`*}
	Example:
	`switch(config-tacacs+)# server 10.10.2.2`
		Configures the TACACS+ server as a member of the TACACS+ server group.
		Tip If the specified TACACS+ server is not found, configure it using the **tacacs-server host** command and retry this command.

Step 4	**`deadtime`** *`minutes`*
	Example:
	`switch(config-tacacs+)# deadtime 30`
		(Optional) Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440.
		Note If the dead-time interval for a TACACS+ server group is greater than zero (0), that value takes precedence over the global dead-time value (see the "Configuring the Dead-Time Interval" section on page 4-23).

Step 5	**`source-interface`** *`interface`*
	Example:
	`switch(config-tacacs+)# source-interface mgmt 0`
		(Optional) Configures a source interface to access the TACACS+ servers in the server group. You can use Ethernet interfaces, loopback interfaces, or the management interface (mgmt 0). The default is the global source interface.

Step 6	**`use-vrf`** *`vrf-name`*
	Example:
	`switch(config-tacacs+)# use-vrf vrf1`
		(Optional) Specifies the VRF to use to contact the servers in the server group.

Step 7	**`exit`**
	Example:
	`switch(config-tacacs+)# exit`
	`switch(config)#`
		Exits TACACS+ server group configuration mode.

Step 8	**`show tacacs-server groups`**
	Example:
	`switch(config)# show tacacs-server groups`
		(Optional) Displays the TACACS+ server group configuration.

Step 9	**`copy running-config startup-config`**
	Example:
	`switch(config)# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Configuring the Global Source Interface for TACACS+ Server Groups

You can configure a global source interface for TACACS+ server groups to use when accessing TACACS+ servers. To configure a different source interface for a specific TACACS+ server group, see the "Configuring TACACS+ Server Groups" section on page 4-14. By default, the Cisco NX-OS software uses any available interface.

Note CFS does not distribute the global TACACS+ source interface configuration.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **ip tacacs source-interface** *interface*
3. **exit**
4. **show tacacs-server directed-request**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	`configure terminal`
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	`switch(config)# ip tacacs source-interface interface`
	Example:
	`switch(config)# ip tacacs source-interface mgmt 0`
		Configures the global source interface for all TACACS+ server groups configured on the device.

Step 3	`exit`
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 4	`show tacacs-server`
	Example:
	`switch# show tacacs-server`
		(Optional) Displays the TACACS+ server configuration information.

Step 5	`copy running-config startup-config`
	Example:
	`switch# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Specifying a TACACS+ Server at Login

You can configure the switch to allow the user to specify which TACACS+ server to send the authentication request by enabling the directed-request option. By default, a Cisco NX-OS device forwards an authentication request based on the default AAA authentication method. If you enable this option, the user can log in as *username@vrfname:hostname,* where *vrfname* is the VRF to use and *hostname* is the name of a configured TACACS+ server.

Note If you enable the directed-request option, the Cisco NX-OS device uses only the TACACS+ method for authentication and not the default local method.

Note User-specified logins are supported only for Telnet sessions.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server directed-request**
3. **show tacacs+** {**pending** | **pending-diff**}
4. **tacacs+ commit**
5. **exit**
6. **show tacacs-server directed-request**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server directed-request** **Example:** `switch(config)# tacacs-server directed-request`	Allows users to specify a TACACS+ server to send the authentication request when logging in. The default is disabled.

Step 3	**show tacacs+** {**pending** | **pending-diff**}
	Example:
	`switch(config)# show tacacs+ distribution pending`
		(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

	Command	Purpose
Step 4	**tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	**show tacacs-server directed-request** **Example:** `switch# show tacacs-server directed-request`	(Optional) Displays the TACACS+ directed request configuration.
Step 7	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the Global TACACS+ Timeout Interval

You can set a global timeout interval that the Cisco NX-OS device waits for responses from all TACACS+ servers before declaring a timeout failure. The timeout interval determines how long the Cisco NX-OS device waits for responses from TACACS+ servers before declaring a timeout failure.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server timeout** *seconds*
3. **show tacacs+** {**pending** | **pending-diff**}
4. **tacacs+ commit**
5. **exit**
6. **show tacacs-server**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server timeout** *seconds* **Example:** `switch(config)# tacacs-server timeout 10`	Specifies the timeout interval for TACACS+ servers. The default timeout interval is 5 seconds. The range is from 1 to 60 seconds.

Step 3	**show tacacs+** {**pending** | **pending-diff**}
	
	Example:
	`switch(config)# show tacacs+ distribution pending`
		(Optional) Displays the TACACS+ configuration pending for distribution (see the“TACACS+ Configuration Distribution” section on page 4-4).

Step 4	**tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

Step 5	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	**show tacacs-server** **Example:** `switch# show tacacs-server`	(Optional) Displays the TACACS+ server configuration.
Step 7	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the Timeout Interval for a Server

You can set a timeout interval that the Cisco NX-OS device waits for responses from a TACACS+ server before declaring a timeout failure. The timeout interval determines how long the Cisco NX-OS device waits for responses from a TACACS+ server before declaring a timeout failure.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the “Enabling TACACS+” section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds*

3. **show tacacs+** {**pending** | **pending-diff**}
4. **tacacs+ commit**
5. **exit**
6. **show tacacs-server**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	`configure terminal`
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	`switch(config)# tacacs-server host {ipv4-address	ipv6-address	host-name} timeout seconds` **Example:** `switch(config)# tacacs-server host server1 timeout 10`	Specifies the timeout interval for a specific server. The default is the global value. **Note** The timeout interval value specified for a TACACS+ server overrides the global timeout interval value specified for all TACACS+ servers.
Step 3	`show tacacs+ {pending	pending-diff}` **Example:** `switch(config)# show tacacs+ pending`	(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

Step 4	`tacacs+ commit`
	Example:
	`switch(config)# tacacs+ commit`
		(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

Step 5	`exit`
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	`show tacacs-server`
	Example:
	`switch# show tacacs-server`
		(Optional) Displays the TACACS+ server configuration.

Step 7	`copy running-config startup-config`
	Example:
	`switch# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Configuring TCP Ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, Cisco NX-OS devices use port 49 for all TACACS+ requests.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port*
3. **show tacacs+** {**pending** | **pending-diff**}
4. **tacacs+ commit**
5. **exit**
6. **show tacacs-server**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* **Example:** `switch(config)# tacacs-server host 10.10.1.1 port 2`	Specifies the TCP port to use for TACACS+ messages to the server. The default TCP port is 49. The range is from 1 to 65535.

Step 3	**show tacacs+** {**pending** | **pending-diff**}
	Example:
	`switch(config)# show tacacs+ distribution pending`
		(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

Step 4	**tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command	Purpose
Step 6	**show tacacs-server** **Example:** `switch# show tacacs-server`	(Optional) Displays the TACACS+ server configuration.
Step 7	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring Periodic TACACS+ Server Monitoring

You can monitor the availability of TACACS+ servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco NX-OS device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.

Note To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

The test idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco NX-OS device sends out a test packet.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Note CFS does not distribute periodic TACACS+ server monitoring configurations.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **tacacs-server dead-time** *minutes*
4. **exit**
5. **show tacacs-server**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
	Example:
	`switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`
		Specifies parameters for server monitoring. The default username is test and the default password is test. The default value for the idle timer is 0 minutes and the valid range is from 0 to 1440 minutes.
		Note For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.

Step 3	**tacacs-server dead-time** *minutes* **Example:** `switch(config)# tacacs-server dead-time 5`	Specifies the number of minutes before the Cisco NX-OS device check a TACACS+ server that was previously unresponsive. The default value is 0 minutes and the valid range is from 0 to 1440 minutes.

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

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

Configuring the Dead-Time Interval

You can configure the dead-time interval for all TACACS+ servers. The dead-time interval specifies the time that the Cisco NX-OS device waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.

Note When the dead-timer interval is 0 minutes, TACACS+ servers are not marked as dead even if they are not responding. You can configure the dead-timer per group (see the "Configuring TACACS+ Server Groups" section on page 4-14).

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server deadtime** *minutes*
3. **show tacacs+** {**pending** | **pending-diff**}
4. **tacacs+ commit**
5. **exit**
6. **show tacacs-server**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server deadtime** *minutes* **Example:** `switch(config)# tacacs-server deadtime 5`	Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes

Step 3	**show tacacs+** {**pending** | **pending-diff**}
	Example:
	`switch(config)# show tacacs+ distribution pending`
		(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

Step 4	**tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	**show tacacs-server** **Example:** `switch# show tacacs-server`	(Optional) Displays the TACACS+ server configuration.
Step 7	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Enabling ASCII Authentication

You can enable ASCII authentication on the TACACS+ server.

Note Only TACACS+ servers support ASCII authentication.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login ascii-authentication**
3. **exit**
4. **show tacacs+** {**pending** | **pending-diff**}
5. **tacacs+ commit**
6. **show aaa authentication login ascii-authentication**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`aaa authentication login ascii-authentication`**
	Example:
	`switch(config)# aaa authentication login ascii-authentication`
		Enables ASCII authentication. The default is disabled.

Step 3	**`show tacacs+`** {**`pending`** | **`pending-diff`**}
	Example:
	`switch(config)# show tacacs+ distribution pending`
		(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

Step 4	**`tacacs+ commit`**
	Example:
	`switch(config)# tacacs+ commit`
		(Optional) Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

Step 5	**`exit`**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command	Purpose
Step 6	**show aaa authentication login ascii-authentication** **Example:** switch# show aaa authentication login ascii-authentication	(Optional) Displays the TACACS+ ASCII authentication configuration.
Step 7	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Committing the TACACS+ Configuration to Distribution

You can apply the TACACS+ global and server configuration stored in the temporary buffer to the running configuration across all NX-OS devices in the fabric (including the originating switch).

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **show tacacs+** {**pending** | **pending-diff**}
3. **tacacs+ commit**
4. **exit**
5. **show tacacs+ distribution status**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**show tacacs+** {**pending** | **pending-diff**} **Example:** switch(config)# show tacacs+ distribution pending	(Optional) Displays the TACACS+ configuration pending for distribution (see the"TACACS+ Configuration Distribution" section on page 4-4).

	Command	Purpose
Step 3	**tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the TACACS+ feature.

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

Step 5	**show tacacs+ distribution status** **Example:** `switch(config)# show tacacs+ distribution status`	(Optional) Displays the TACACS distribution configuration and status.
Step 6	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Discarding the TACACS+ Distribution Session

You can discard the temporary database of TACACS+ changes and end the CFS distribution session.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the “Enabling TACACS+” section on page 4-8).

SUMMARY STEPS

1. **configure terminal**
2. **show tacacs+** {**pending** | **pending-diff**}
3. **tacacs+ abort**
4. **exit**
5. **show tacacs+ distribution status**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**show tacacs+** {**pending** | **pending-diff**} **Example:** switch(config)# show tacacs+ distribution pending	(Optional) Displays the TACACS+ configuration pending for distribution (see the“TACACS+ Configuration Distribution” section on page 4-4).
Step 3	**tacacs+ abort** **Example:** switch(config)# tacacs+ abort	Discards the TACACS+ configuration in the temporary storage and ends the session.
Step 4	**exit** **Example:** switch(config)# exit switch#	Exits configuration mode.
Step 5	**show tacacs+ distribution status** **Example:** switch(config)# show tacacs+ distribution status	(Optional) Displays the TACACS distribution configuration and status.

Clearing the TACACS+ Distribution Session

You can clear an active CFS distribution session and unlock TACACS+ configuration in the network.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the “Enabling TACACS+” section on page 4-8).

SUMMARY STEPS

1. **clear tacacs+ session**
2. **show tacacs+ distribution status**

DETAILED STEPS

	Command	Purpose

Step 1	**`clear tacacs+ session`**
	Example:
	`switch# clear tacacs+ session`
		Clears the CFS session for TACACS+ and unlocks the fabric.

Step 2	**`show tacacs+ distribution status`**
	Example:
	`switch(config)# show tacacs+ distribution status`
		(Optional) Displays the TACACS distribution configuration and status.

Manually Monitoring TACACS+ Servers or Groups

You can manually issue a test message to a TACACS+ server or to a server group.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. **test aaa group** *group-name username password*

DETAILED STEPS

	Command	Purpose

Step 1	**`test aaa server tacacs+`** {*`ipv4-address`* | *`ipv6-address`* | *`host-name`*} [**`vrf`** *`vrf-name`*] *`username password`*
	Example:
	`switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH`
		Sends a test message to a TACACS+ server to confirm availability.

Step 2	**`test aaa group`** *`group-name username password`*
	Example:
	`switch# test aaa group TacGroup user2 As3He3CI`
		Sends a test message to a TACACS+ server group to confirm availability.

Disabling TACACS+

You can disable TACACS+.

Caution When you disable TACACS+, all related configurations are automatically discarded.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. **configure terminal**
2. **no feature tacacs+**
3. **exit**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`no feature tacacs+`**
	Example:
	`switch(config)# no feature tacacs+`
		Disables TACACS+.

Step 3	**`exit`**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 4	**`copy running-config startup-config`**
	Example:
	`switch# copy running-config`
	`startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Displaying TACACS+ Statistics

You can display the statistics that the Cisco NX-OS device maintains for TACACS+ activity.

BEFORE YOU BEGIN

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

Enable TACACS+ (see the "Enabling TACACS+" section on page 4-8).

SUMMARY STEPS

1. **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command	Purpose

Step 1	`switch#` **`show tacacs-server statistics`**
	`{`*`hostname`*` | `*`ipv4-address`*` | `*`ipv6-address`*`}`
	
	`Example:`
	`switch# show tacacs-server statistics 10.10.1.1`
		Displays the TACACS+ statistics.

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

Verifying TACACS+ Configuration

To display TACACS+ configuration information, perform one of the following tasks:

Command	Purpose
show feature	Displays the enabled status of the feature.
show tacacs+ {**status** | **pending** | **pending-diff**}	Displays the TACACS+ Cisco Fabric Services distribution status and other details.
show running-config tacacs [**all**]	Displays the TACACS+ configuration in the running configuration.
show startup-config tacacs	Displays the TACACS+ configuration in the startup configuration.
show tacacs-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	Displays all configured TACACS+ server parameters.

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

Example TACACS+ Configurations

The following example shows how to configure TACACS+:

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
    server 10.10.2.2
```

Where to Go Next

You can now configure AAA authentication methods to include the TACACS+ server groups (see Chapter 2, "Configuring AAA").

Default Settings

Table 4-1 lists the default settings for TACACS+ parameters.

Table 4-1 Default TACACS+ Parameters

Parameters	Default
TACACS+	Disabled
Dead timer interval	0 minutes
Timeout interval	5 seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test

Additional References

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

- Related Documents, page 4-32
- Standards, page 4-32
- MIBs, page 4-33

Related Documents

Related Topic	Document Title
NX-OS 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-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/enigmatic/cant/mibs.shtml

Feature History for TACACS+

Table 4-2 lists the release history for this feature.

Table 4-2 Feature History for TACACS+

Feature Name	Releases	Feature Information
CFS support	4.1(2)	Added CFS distribution for the TACACS+ configuration on the Cisco NX-OS device.
ASCII authentication for passwords	4.1(2)	Added ability to enable ASCII authentication on TACACS+ servers.
TACACS+	4.0(1)	This feature was introduced.