CHAPTER 5

Configuring TACACS+

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol for the Nexus 1000V.

You can use TACACS+ to provide centralized validation of users attempting to gain access to a 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 device are available.

Note The logging level for TACACS + must be set to 5. Use the command-line interface (CLI) to set the logging level.

This chapter includes the following sections:

Information About TACACS+

The TACACS+ security protocol provides centralized validation of users attempting to gain access to a 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 device are available.

TACACS+ provides for separate authentication, authorization, and accounting services. The TACACS+ daemon provides each service 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. Centralized authentication is provided using the TACACS+ protocol.

This section includes the following topics:

TACACS+ Operation for User Login

THe following sequence of events take place when you attempt to login to a TACACS+ server using Password Authentication Protocol (PAP):

1. When a connection is established, the TACACS+ daemon is contacted 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 additional information, such as mother's maiden name.

2. The TACACS+ daemon provides one of the following responses:
   a. ACCEPT—User authentication succeeds and service begins. If user authorization is needed, 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. If an ERROR response is received, the device tries to use an alternative method for authenticating the user.

   If further authorization is required after authentication, the user also undergoes an additional authorization phase. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
3. If TACACS+ authorization is required, the TACACS+ daemon is contacted 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, access list, and user timeouts

Default TACACS+ Server Encryption Type and Preshared Key

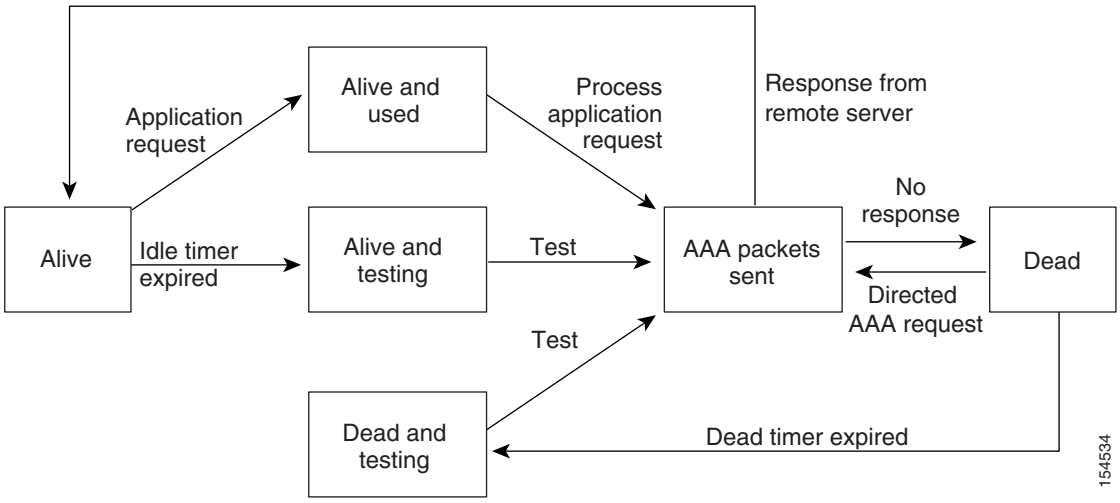
You must configure the TACACS+ preshared key to authenticate to the TACACS+ server. A preshared key is a secret text string shared between the device and the TACACS+ server host. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not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

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

TACACS+ Server Monitoring

Unresponsive TACACS+ servers are marked as dead and are not sent AAA requests. Dead TACACS+ servers are periodically monitored and brought back alive once they respond. This process confirms that a TACACS+ server is in a working state before real AAA requests are sent its way. The following figure shows how a TACACS+ server state change generates a Simple Network Management Protocol (SNMP) trap and an error message showing the failure before it impacts performance.

Figure 5-1 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.

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.

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, 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 are supported VSA protocol options:

- 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.

Thefollowing are other supported attributes:

- roles—Lists all the roles to which the user belongs. The value consists of a string listing the role names delimited by white space. 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.
- 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).

Prerequisites for TACACS+

TACACS+ has the following prerequisites:

- Obtain the IP addresses or hostnames for the TACACS+ servers.
- Obtain the preshared keys from the TACACS+ servers, if any.
- Ensure that the Nexus 1000V is configured as a TACACS+ client of the AAA servers.
- You have already configured AAA, including remote TACACS+ authentication using the following procedures:
  - Configuring a Login Authentication Method, page 3-6
  - Verifying AAA Configuration, page 3-8

Guidelines and Limitations

TACACS+ has the following guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers.

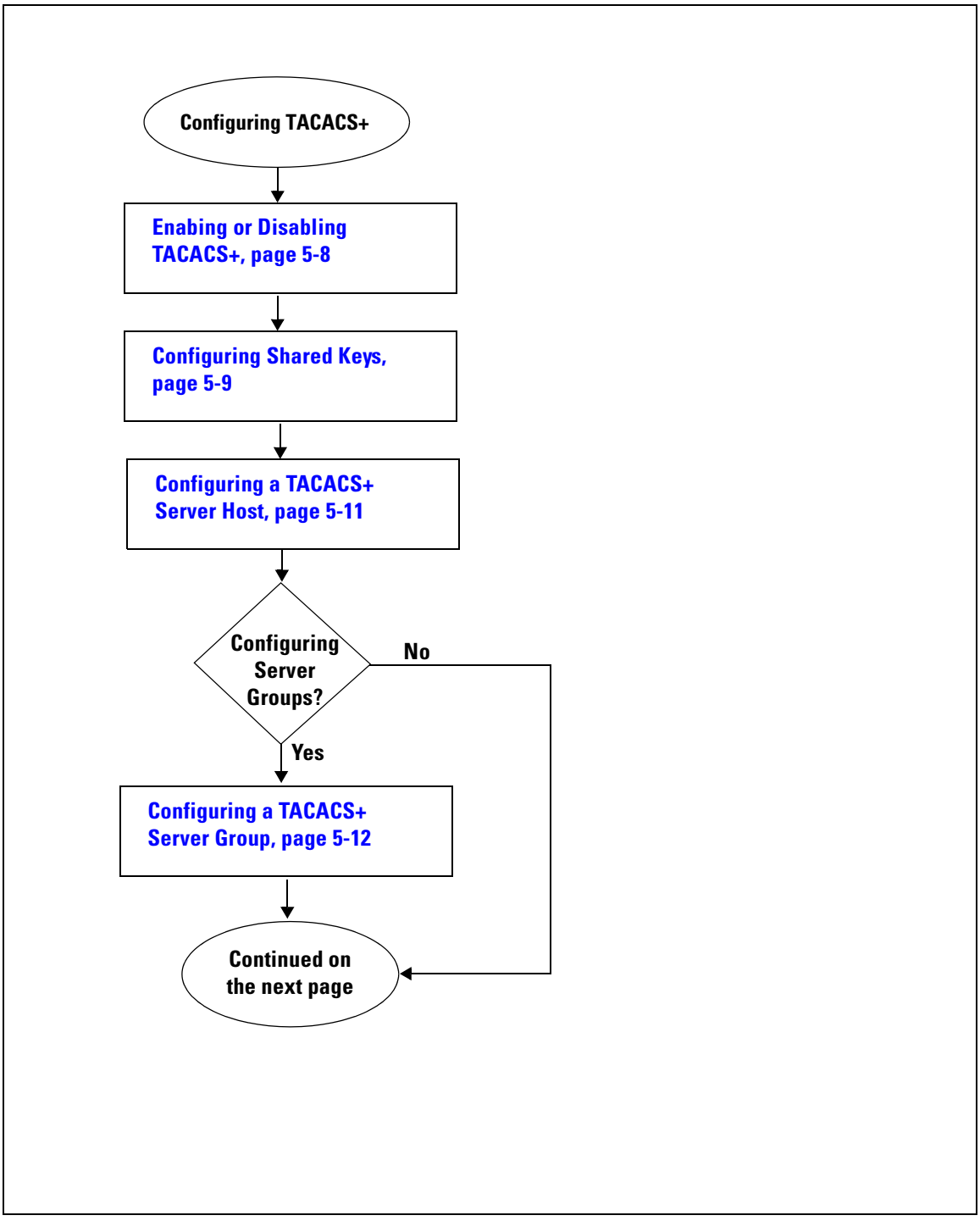
Configuring TACACS+

This section includes the following topics:

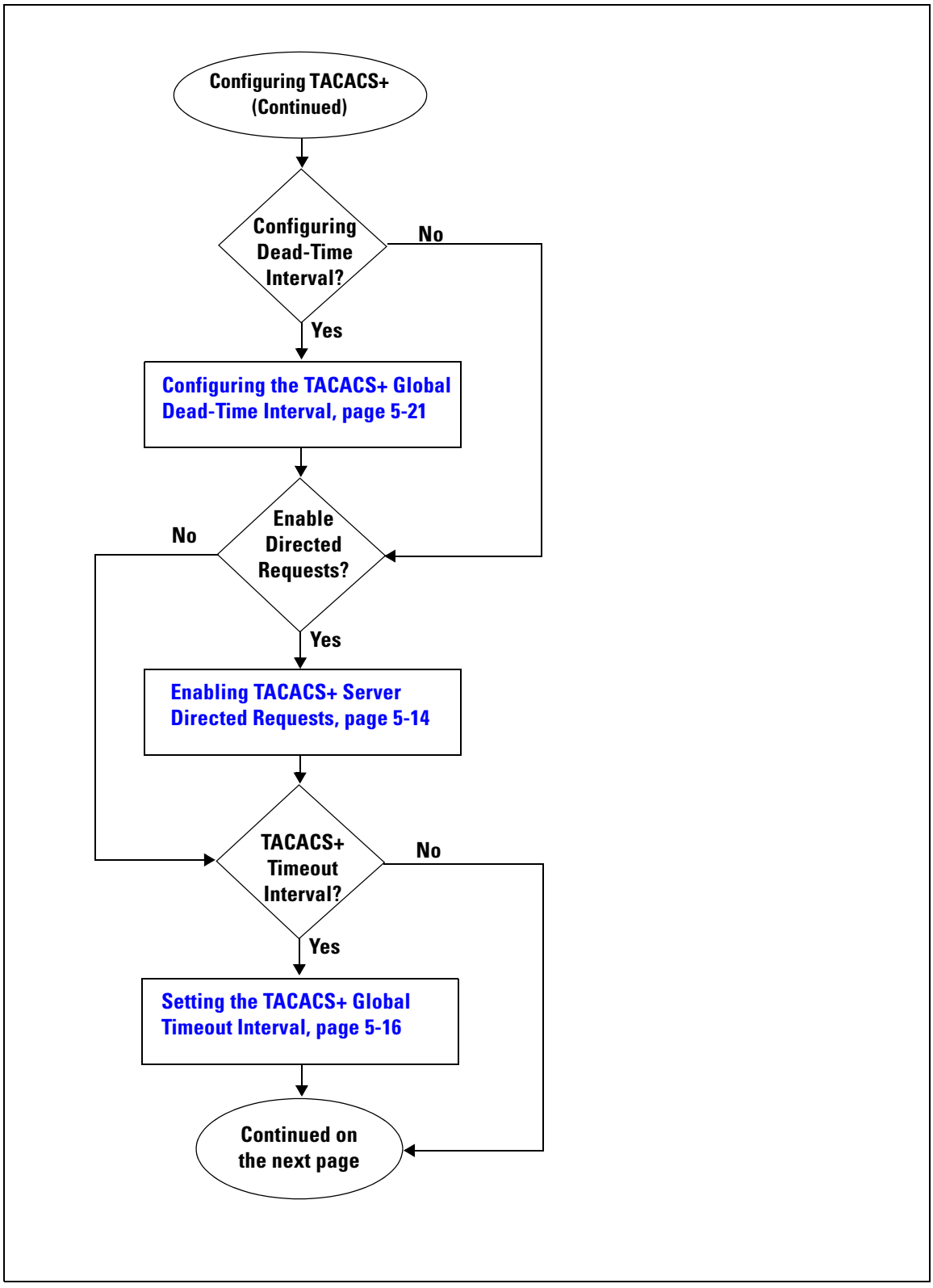
Note Be aware that the Nexus 1000V commands may differ from the Cisco IOS commands.

Use the following flow chart to configure TACACS+.

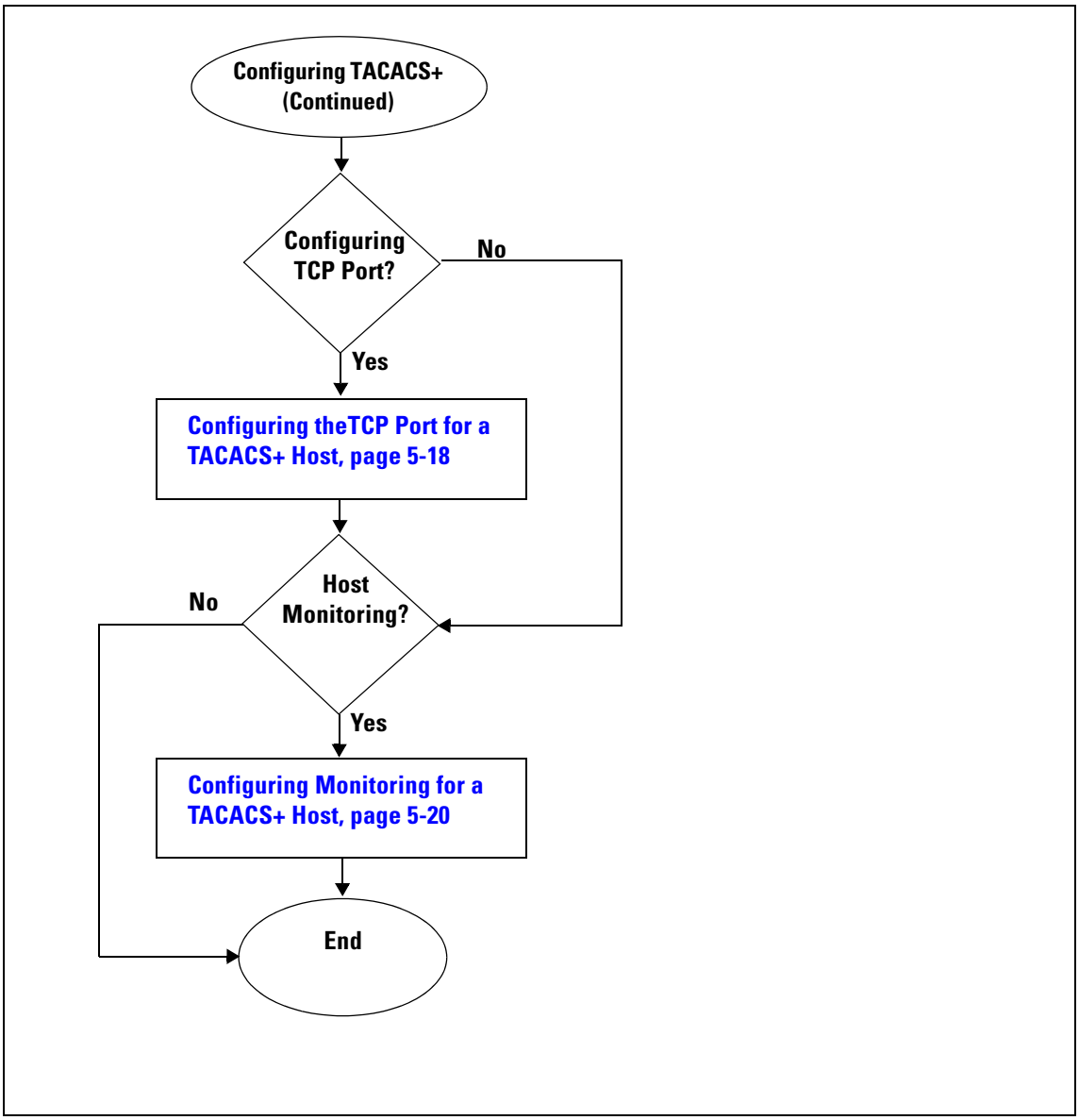
Flow Chart: Configuring TACACS+



Flow Chart: Configuring TACACS+ (Continued)



Flow Chart: Configuring TACACS+ (Continued)



Enabing or Disabling TACACS+

Use this procedure to either enable or disable TACACS+.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following.

- You are logged in to the CLI in EXEC mode.
- By default, TACACS+ is disabled. You must explicitly enable the TACACS+ feature to access the configuration and verification commands that support TACACS+ authentication.

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

SUMMARY STEPS

1. **config t**
2. **[no] tacacs+ enable**
3. **exit**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	**[no] tacacs+ enable** **Example:** n1000v(config)# tacacs+ enable n1000v(config)# **Example:** n1000v(config)# no tacacs+ enable n1000v(config)#	Enables or disables TACACS+.
Step 3	**exit** **Example:** n1000v(config)# exit n1000v#	Exits the CLI Global Configuration mode and returns you to EXEC mode.
Step 4	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Copies the changes you made to the startup configuration.

Configuring Shared Keys

Use this procedure to configure the following:

- The global key, or a secret text string shared between the Nexus 1000V and all TACACS+ server hosts
- The key, or secret text string shared between the Nexus 1000V and a single TACACS+ server host

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabling or Disabling TACACS+" procedure on page 5-8.
- You know the key for the TACACS+ server host(s).
- By default, no global key is configured.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	Do one of the following: • To configure a global key for all TACACS+ server hosts, continue with the next step. • To configure a key for a single TACACS+ server host, go to Step 5.	

Step 3	**tacacs-server key** [**0** | **7**] *global_key*
	
	Example:
	`n1000v(config)# tacacs-server key 0 QsEFtkI#`
	`n1000v(config)#`
		Designates the global key shared between the Nexus 1000V and the TACACS+ server hosts.
		0: Specifies a clear text string (key) to follow. [the default]
		7: Specifies an encrypted string (key) to follow.
		global_key: A string of up to 63 characters.
		By default, no global key is configured.

Step 4	Go to Step 6.	

Step 5	**tacacs-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *shared_key*
	
	Example:
	`n1000v(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg`
	`n1000v(config)#`
		Designates the key shared between the Nexus 1000V and this specific TACACS+ server host.
		0: Specifies a clear text string (key) to follow. [the default]
		7: Specifies an encrypted string (key) to follow.
		global_key: A string of up to 63 characters.
		This shared key is used instead of the global shared key.

	Command	Purpose

Step 6	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits the CLI Global Configuration mode and returns you to EXEC mode.

Step 7	**show tacacs-server**
	
	Example:
	`n1000v# show tacacs-server`
	`Global TACACS+ shared secret:********`
	`timeout value:5`
	`deadtime value:0`
	`total number of servers:1`
	
	`following TACACS+ servers are configured:`
	`10.10.2.2:`
	`available on port:49`
		(Optional) Displays the TACACS+ server configuration.
		
		Note The global shared key is saved in encrypted form in the running configuration. To dsiplay the key, use the **show running-config** command.

Step 8	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies these changes in the running configuration to the startup configuration.

Configuring a TACACS+ Server Host

Use this procedure to configure a TACACS+ server as a TACACS+ host.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabing or Disabling TACACS+" procedure on page 5-8.
- You have already configured the shared key, using the following:

  "Configuring Shared Keys" procedure on page 5-9
- You know the IP addresses or the hostnames for the remote TACACS+ server hosts.
- All TACACS+ server hosts are added to the default TACACS+ server group.

SUMMARY STEPS

1. **config t**
2. **tacacs-server host** {*ipv4-address* | *host-name*}
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	**tacacs-server host** {*ipv4-address* | *host-name*} **Example:** n1000v(config)# tacacs-server host 10.10.2.2	Configures the server IP address or hostname as a TACACS+ server host.
Step 3	**exit** **Example:** n1000v(config)# exit n1000v#	Exits the CLI Global Configuration mode and returns you to EXEC mode.
Step 4	**show tacacs-server** **Example:** n1000v# **show tacacs-server** timeout value:5 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:49 n1000v#	(Optional) Displays the TACACS+ server configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Copies these changes in the running configuration to the startup configuration.

Configuring a TACACS+ Server Group

Use this procedure to configure a TACACS+ server group whose member servers share authentication functions.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- All servers added to a TACACS+ server group must use the TACACS+ protocol.
- Once the TACACS+ server group is configured, the server members are tried in the same order in which you configured them.
- You have already enabled TACACS+ for authentication.
  See the "Enabling or Disabling TACACS+" procedure on page 5-8.

- You have already configured the preshared keys, using the following:

  "Configuring Shared Keys" procedure on page 5-9

- A TACACS+ server group can provide fail-over in case one server fails to respond. If the first server in the group fails, the next server in the group is tried until a server responds. Multiple server groups can provide fail-over for each other in this same way.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**aaa group server tacacs+** *group-name*
	
	Example:
	`n1000v(config)# aaa group server tacacs+ TacServer`
	`n1000v(config-tacacs+)#`
		Creates a TACACS+ server group with the specified name and paces you into the TACACS+ configuration mode for that group.

Step 3	**server** {*ipv4-address* | *host-name*}
	
	Example:
	`n1000v(config-tacacs+)# server 10.10.2.2`
	`n1000v(config-tacacs+)#`
		Configures the TACACS+ server host-name or IP address 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:
	`n1000v(config-tacacs+)# deadtime 30`
	`n1000v(config-tacacs+)#`
		(Optional) Configures the monitoring dead time for this TACACS+ group. The default is 0 minutes. The range is from 0 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 TACACS+ Global Dead-Time Interval" procedure on page 5-21).

	Command	Purpose
Step 5	**use-vrf** *vrf-name* **Example:** n1000v(config-tacacs+)# use-vrf management n1000v(config-tacacs+)#	(Optional) Specifies the virtual routing and forwarding instance (VRF) to use to contact this server group.
Step 6	**exit** **Example:** n1000v(config-tacacs+)# exit n1000v(config)#	Exits the TACACS+ Configuration mode and returns you to Global Configuration mode.
Step 7	**exit** **Example:** n1000v(config)# exit n1000v#	Exits the Global Configuration mode and returns you to EXEC mode.
Step 8	**show tacacs-server groups** **Example:** n1000v# show tacacs-server groups total number of groups:1 following TACACS+ server groups are configured: group TacServer: server 10.10.2.2 on port 49 deadtime is 30 vrf is management n1000v#	(Optional) Displays the TACACS+ server group configuration.
Step 9	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	(Optional) Copies these changes made in the running configuration to the startup configuration.

Example:
```
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-tacacs+)# server 10.10.2.2
n1000v(config-tacacs+)# deadtime 30
n1000v(config-tacacs+)# use-vrf management
n1000v(config-tacacs+)# exit
n1000v(config)# exit
n1000v# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 30
                vrf is management
n1000v#
```

Enabling TACACS+ Server Directed Requests

Use this procedure to let users designate the TACACS+ server to send their authentication request to. This is called a directed-request.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabing or Disabling TACACS+" procedure on page 5-8.

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

- When directed requests are enabled, 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.

SUMMARY STEPS

1. **config t**
2. **tacacs-server directed-request**
3. **exit**
4. **show tacacs-server directed-request**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**tacacs-server directed-request**
	
	Example:
	`n1000v(config)# tacacs-server directed-request`
	`n1000v(config)#`
		Enables use of directed requests for specifying the TACACS+ server to send an authentication request to when logging in. The default is disabled.

Step 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits the CLI Global Configuration mode and returns you to EXEC mode.

Step 4	**show tacacs-server directed-request**
	
	Example:
	`n1000v# show tacacs-server directed-request`
	`enabled`
	`n1000v#`
		(Optional) Displays the TACACS+ directed request configuration.

Step 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Setting the TACACS+ Global Timeout Interval

Use this procedure to set the interval in seconds that the Nexus 1000V waits for a response from any TACACS+ server before declaring a timeout.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabing or Disabling TACACS+" procedure on page 5-8.
- The timeout specified for an individual TACACS+ server overrides the global timeout interval. To set the timeout for an individual server, see the "Setting a Timeout Interval for an Individual TACACS+ Host" procedure on page 5-17.

SUMMARY STEPS

1. **config t**
2. **tacacs-server timeout** *seconds*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**tacacs-server timeout** *seconds* **Example:** `n1000v(config)# tacacs-server timeout 10`	Specifies the interval in seconds that the Nexus 1000V waits for a response from a server. The default timeout interval is 5 seconds. The range is from 1 to 60 seconds.

Step 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits the CLI Global Configuration mode and returns you to EXEC mode.

	Command	Purpose

Step 4	**show tacacs-server**
	
	Example:
	`n1000v# show tacacs-server`
	`Global TACACS+ shared secret:********`
	`timeout value:10`
	`deadtime value:0`
	`total number of servers:1`
	
	`following TACACS+ servers are configured:`
	`10.10.2.2:`
	`available on port:49`
	`n1000v#`
		(Optional) Displays the TACACS+ server configuration.

Step 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies these changes made in the running configuration to the startup configuration.

Setting a Timeout Interval for an Individual TACACS+ Host

Use this procedure to set the interval in seconds that the Nexus 1000V waits for a response from a specific TACACS+ server before declaring a timeout. This setting is configured per TACACS+ host.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabing or Disabling TACACS+" procedure on page 5-8.
- The timeout setting for an individual TACACS+ server overrides the global timeout interval.

SUMMARY STEPS

1. **config t**
2. **tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	**tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds* **Example:** n1000v(config)# tacacs-server host 10.10.2.2 timeout 10 n1000v(config)#	Specifies the timeout interval for a specific server. The default is the global timeout interval. For more information, see the "Setting the TACACS+ Global Timeout Interval" procedure on page 5-16.
Step 3	**exit** **Example:** n1000v(config)# exit n1000v#	Exits the CLI Global Configuration mode and returns you to EXEC mode.
Step 4	**show tacacs-server** **Example:** n1000v# show tacacs-server Global TACACS+ shared secret:******** timeout value:10 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:49 timeout:10 n1000v#	(Optional) Displays the TACACS+ server configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Copies these changes made in the running configuration to the startup configuration.

Configuring theTCP Port for a TACACS+ Host

Use this procedure to configure a TCP port other than port 49 (the default for TACACSS+ requests).

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabing or Disabling TACACS+" procedure on page 5-8.
- You have configured the TACACS+ server using the "Configuring a TACACS+ Server Host" procedure on page 5-11.

SUMMARY STEPS

1. **config t**
2. **tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	**tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port* **Example:** n1000v(config)# tacacs-server host 10.10.2.2 port 2 n1000v(config)#	Specifies the TCP port to use. allowable range: 1 to 65535 default: 49
Step 3	**exit** **Example:** n1000v(config)# exit n1000v#	Exits the CLI Global Configuration mode and returns you to EXEC mode.
Step 4	**show tacacs-server** **Example:** n1000v# show tacacs-server Global TACACS+ shared secret:******** timeout value:10 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:2 timeout:10 n1000v#	(Optional) Displays the TACACS+ server configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring Monitoring for a TACACS+ Host

Use this procedure to configure periodic monitoring of a TACACS+ host.

BEFORE YOU BEGIN

Before starting this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabling or Disabling TACACS+" procedure on page 5-8.
- You have configured the TACACS+ server.
  See the "Configuring a TACACS+ Server Host" procedure on page 5-11.
- The idle timer specifies how long a TACACS+ server should remain idle (receiving no requests) before sending it a test packet.
- The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not done.

SUMMARY STEPS

1. **config t**
2. **tacacs-server host** {*ipv4-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	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**tacacs-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `n1000v(config)# tacacs-server host 10.10.2.2 test username pvk2 password a3z9yjqz7 idle-time 3`	Configures server monitoring. **username**: The default is test. **Note** To protect network security, we recommend assigning a username that is not already in the TACACS+ database. **password**: The default is test. **idle-time**: The default is 0 minutes. The valid range is from 0 to 1440 minutes. **Note** For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.

	Command	Purpose
Step 3	**tacacs-server dead-time** *minutes* **Example:** `n1000v(config)# tacacs-server dead-time 5`	Specifies the duration of time in minutes before checking 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:
	`n1000v(config)# exit`
	`n1000v#`
		Exits the CLI Global Configuration mode and returns you to EXEC mode.

Step 5	**show tacacs-server**
	
	Example:
	`n1000v# show tacacs-server`
	`Global TACACS+ shared secret:********`
	`timeout value:10`
	`deadtime value:0`
	`total number of servers:1`
	
	`following TACACS+ servers are configured:`
	`10.10.2.2:`
	`available on port:2`
	`timeout:10`
	`n1000v#`
		(Optional) Displays the TACACS+ server configuration.

Step 6	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies these changes made to the running configuration to the startup configuration.

Configuring the TACACS+ Global Dead-Time Interval

Use this procedure to configure the interval to wait before sending a test packet to a previously unresponsive server.

BEFORE YOU BEGIN

Before starting this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabing or Disabling TACACS+" procedure on page 5-8.
- You have configured the TACACS+ server.
  See the "Configuring a TACACS+ Server Host" procedure on page 5-11.
- 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 a TACACS+ Server Group" procedure on page 5-12).

SUMMARY STEPS

1. **config t**
2. **tacacs-server deadtime** *minutes*
3. **exit**

4. **show tacacs-server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**tacacs-server deadtime** *minutes* **Example:** `n1000v(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	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits the CLI Global Configuration mode and returns you to EXEC mode.

Step 4	**show tacacs-server** **Example:** `n1000v# show tacacs-server`	(Optional) Displays the TACACS+ server configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Displaying Statistics for a TACACS+ Host

Use this procedure to display the statistics for TACACS+ host.

BEFORE YOU BEGIN

Before starting this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already enabled TACACS+ for authentication.
  See the "Enabing or Disabling TACACS+" procedure on page 5-8.
- You have configured the TACACS+ server.
  See the "Configuring a TACACS+ Server Host" procedure on page 5-11.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**show tacacs-server statistics** {*hostname* | *ipv4-address*}	Displays statistics for a TACACS+ host.

Example:

```
n1000v# show tacacs-server statistics 10.10.1.1
Server is not monitored

Authentication Statistics
        failed transactions: 9
        sucessfull transactions: 2
        requests sent: 2
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Authorization Statistics
        failed transactions: 1
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Example TACACS+ Configuration

The following example shows a TACACS+ configuration:

```
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
```

Default Settings

The following table lists the default settings for 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

Feature History for TACACS+

This section provides the TACACS+ release history.

Feature Name	Releases	Feature Information
TACACS+	4.0	This feature was introduced.

Additional References

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

Related Documents

Related Topic	Document Title
CLI	*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)*
System Management	*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(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.	—