

Send comments to nexus5k-docfeedback@cisco.com



T Commands

This chapter describes the Cisco NX-OS security commands that begin with T.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

tacacs-server deadline

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadline** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadline *minutes*

no tacacs-server deadline *minutes*

Syntax Description	<i>time</i>	Time interval in minutes. The range is from 1 to 1440.
---------------------------	-------------	--

Command Default	0 minutes
------------------------	-----------

Command Modes	Global configuration mode
----------------------	---------------------------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines	Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.
-------------------------	---

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples	This example shows how to configure the dead-time interval and enable periodic monitoring:
-----------------	--

```
switch(config)# tacacs-server deadline 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
switch(config)# no tacacs-server deadline 10
```

Related Commands	Command	Description
	deadline	Sets a dead-time interval for monitoring a nonresponsive RADIUS or TACACS+ server group.
	feature tacacs+	Enables TACACS+.
	show tacacs-server	Displays TACACS+ server information.

Send comments to nexus5k-docfeedback@cisco.com

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **tacacs-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description This command has no arguments or keywords.

Command Default Sends the authentication request to the configured TACACS+ server groups.

Command Modes Global configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines You must use the **feature tacacs+** command before you configure TACACS+. During login, the user can specify the *username@vrfname:hostname*, where *vrfname* is the VRF to use and *hostname* is the name of a configured TACACS+ server. The username is sent to the server name for authentication.

Examples This example shows how to allow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch(config)# tacacs-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch(config)# no tacacs-server directed-request
```

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
	show tacacs-server directed request	Displays a directed request TACACS+ server configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command. To revert to the defaults, use the **no** form of this command.

```
tacacs-server host {hostname | ipv4-address | ipv6-address} [key [0 | 7] shared-secret]
[port port-number] [test {idle-time time | password password | username name}]
[timeout seconds]
```

```
no tacacs-server host {hostname | ipv4-address | ipv6-address} [key [0 | 7] shared-secret]
[port port-number] [test {idle-time time | password password | username name}]
[timeout seconds]
```

Syntax Description

<i>hostname</i>	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
<i>ipv4-address</i>	TACACS+ server IPv4 address in the <i>A.B.C.D</i> format.
<i>ipv6-address</i>	TACACS+ server IPv6 address in the <i>X:X:X::X</i> format.
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
<i>shared-secret</i>	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.
port <i>port-number</i>	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time <i>time</i>	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password <i>password</i>	(Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username <i>name</i>	(Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout <i>seconds</i>	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Send comments to nexus5k-docfeedback@cisco.com

Command Default

Idle time: disabled.
 Server monitoring: disabled.
 Timeout: 1 second.
 Test username: test.
 Test password: test.

Command Modes

Global configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.
 When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Examples

This example shows how to configure TACACS+ server host parameters:

```
switch(config)# tacacs-server host 192.168.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 192.168.2.3 test idle-time 10
switch(config)# tacacs-server host 192.168.2.3 test username tester
switch(config)# tacacs-server host 192.168.2.3 test password 2B9ka5
```

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
	show tacacs-server	Displays TACACS+ server information.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To remove a configured shared secret, use the **no** form of this command.

```
tacacs-server key [0 | 7] shared-secret
```

```
no tacacs-server key [0 | 7] shared-secret
```

Syntax Description	0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
	7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
	<i>shared-secret</i>	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines You must configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples This example shows how to display configure TACACS+ server shared keys:

```
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
	show tacacs-server	Displays TACACS+ server information.

Send comments to nexus5k-docfeedback@cisco.com

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To revert to the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description	<i>seconds</i>	Seconds between retransmissions to the TACACS+ server. The valid range is 1 to 60 seconds.
---------------------------	----------------	--

Command Default	1 second
------------------------	----------

Command Modes	Global configuration mode
----------------------	---------------------------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines	You must use the feature tacacs+ command before you configure TACACS+.
-------------------------	---

Examples	This example shows how to configure the TACACS+ server timeout value:
-----------------	---

```
switch(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
switch(config)# no tacacs-server timeout 3
```

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.	

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

telnet

To create a Telnet session using IPv4 on a Cisco Nexus 5000 Series switch, use the **telnet** command.

```
telnet {ipv4-address | hostname} [port-number] [vrf {vrf-name | default | management}]
```

Syntax Description		
<i>ipv4-address</i>		IPv4 address of the remote switch.
<i>hostname</i>		Hostname of the remote switch. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
<i>port-number</i>		(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf <i>vrf-name</i>		(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default		Specifies the default VRF.
management		Specifies the management VRF.

Command Default Port 23 is the default port.

Command Modes EXEC mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines To create a Telnet session with IPv6 addressing, use the **telnet6** command.

Examples This example shows how to start a Telnet session using IPv4:

```
switch# telnet 192.168.1.1 vrf management
switch#
```

Related Commands	Command	Description
	clear line	Clears Telnet sessions.
	telnet server enable	Enables the Telnet server.
	telnet6	Creates a Telnet session using IPv6 addressing.

Send comments to nexus5k-docfeedback@cisco.com

telnet server enable

To enable the Telnet server, use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

telnet server enable

no telnet server enable

Syntax Description This command has no arguments or keywords.

Command Default Enable

Command Modes Global configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to enable the Telnet server:

```
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch(config)# no telnet server enable
```

Related Commands	Command	Description
	show telnet server	Displays the Telnet server status.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

telnet6

To create a Telnet session using IPv6 on the Cisco NX-OS switch, use the **telnet6** command.

```
telnet6 {ipv6-address | hostname} [port-number] [vrf {vrf-name | default | management}]
```

Syntax Description		
<i>ipv6-address</i>		IPv6 address of the remote device.
<i>hostname</i>		Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
<i>port-number</i>		(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf <i>vrf-name</i>		(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default		Specifies the default VRF.
management		Specifies the management VRF.

Command Default Port 23 is the default port. The default VRF is used.

Command Modes EXEC mode

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the Telnet server using the **telnet server enable** command. To create a Telnet session with IPv4 addressing, use the **telnet** command.

Examples This example shows how to start a Telnet session using an IPv6 address:

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
switch#
```

Related Commands	Command	Description
	clear line	Clears Telnet sessions.
	telnet	Creates a Telnet session using IPv4 addressing.
	telnet server enable	Enables the Telnet server.