tacacs-server administration through title-color

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server**command in global configuration mode. To remove the configuration, use the **no** form of this command.

tacacs server *name*

no tacacs server

Syntax Description

name	Name of the private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

Related Commands

Command	Description
address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.

Command	Description
send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
single-connection **(TACACS+)**	Enables all TACACS packets to be sent to the same server using a single TCP connection.
timeout **(TACACS+)**	Configures the time to wait for a reply from the specified TACACS server.

tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no**form of this command.

tacacs-server host{*host-name*| *host-ip-address*}[**key***string*][**[nat]**[**port**[*integer*]]**[single-connection]**[**timeout**[*integer*]]]

no tacacs-server host{*host-name*| *host-ip-address*}

Syntax Description

host-name	Name of the host.
host-ip-address	IP address of the host.
key	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command **tacacs-server key**for this server only.
string	(Optional) Character string specifying authentication and encryption key.
nat	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.
port	(Optional) Specifies a TACACS+ server port number. This option overrides the default, which is port 49.
integer	(Optional) Port number of the server. Valid port numbers range from 1 through 65535.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
timeout	(Optional) Specifies a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
integer	(Optional) Integer value, in seconds, of the timeout interval. The value is from 1 through 1000.

Command Default

No TACACS+ host is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	The **nat** keyword was added.
12.2(8)T	The **nat** keyword was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **port**, **timeout**, **key, single-connection, and nat**keywords only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

The **single-connection** keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

Examples

The following example specifies a TACACS+ host named Sea_Change:

```
tacacs-server host Sea_Change
```

The following example specifies that, for authentication, authorization, and accounting (AAA) confirmation, the router consults the TACACS+ server host named Sea_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a_secret.

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
aaa authentication	Specifies or enables AAA authentication.
aaa authorization	Sets parameters that restrict user access to a network.
aaa accounting	Enables AAA accounting of requested services for billing or security.
ppp	Starts an asynchronous connection using PPP.

Command	Description
slip	Starts a serial connection to a remote host using SLIP.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

Syntax Description

host	A hostname or an IP address.
port	(Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host.
keyword	(Optional) One of the keywords listed in the table below.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The **/ipv4** and **/ipv6** keywords were added.
12.1	The **/quiet** keyword was added.
12.2(2)T	The **/ipv4** and **/ipv6** keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The table below lists the optional **telnet** command keywords.

Table 1: telnet Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/ipv4	Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/ipv6	Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the **Enter** key. You can edit the line using the standard Cisco IOS software command-editing characters. The **/line** keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route: *path*	Specifies loose source routing. The *path* argument is a list of hostnames or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.

Option	Description
/stream	Turns on *stream* processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
port-number	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd *rcmd*	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.

Option	Description
pim-auto-rp	Protocol Independent Multicast (PIM) auto-rendezvous point (RP).
node	Connect to a specific Local-Area Transport (LAT) node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination local-area transport (LAT) port name.
smtp	Simple Mail Transfer Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specifies TACACS security.
talk	Talk (517).
telnet	Telnet (23).
time	Time (37).
uucp	UNIX-to-UNIX Copy Program (540).
whois	Nickname (43).
www	World Wide Web (HTTP, 80).

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned hostname--as long as the following conditions are met:

- The hostname is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use, or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. The table below lists the special Telnet escape sequences.

Table 2: Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP and IPv6)
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

1 The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt: **Ctrl-^ ?**

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router>

telnet host1 /encrypt kerberos
```

The following example routes packets from the source system host1 to example.com, then to 10.1.0.11, and finally back to *host1* :

```
router>
telnet host1 /route:example.com 10.1.0.11 host1
```

The following example connects to a host with the logical name host1:

```
router>
host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router>

telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32
Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
name connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
show tcp	Displays the status of TCP connections.

test aaa group

To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile with the record that is sent to the RADIUS server or to manually test load-balancing server status, use the **test aaa group** command in privileged EXEC mode.

DNIS and CLID User Profile

test aaa group {*group-name*| **radius**} *username password* **new-code** [**profile** *profile-name*]

RADIUS Server Load Balancing Manual Testing

test aaa group *group-name* [**server** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] *username password* **new-code** [**count** *requests*] [**rate** *requests-per-second*] [**blocked** {**yes**| **no**}]

Syntax Description

group-name	Subset of RADIUS servers that are used, as defined by the server group group-name.
radius	Uses RADIUS servers for authentication.
username	Name for the test user. **Caution** If you use this command to manually test RADIUS load-balancing server state, it is recommended that a test user, one that is not defined on the RADIUS server, be used to protect against security issues that may arise if the test user is not correctly configured.
password	Password.
new-code	Code path through the new code, which supports a CLID or DNIS user profile association with a RADIUS server.
profile *profile-name*	(Optional) Identifies the user profile specified in the aaa user profile command. To associate a user profile with the RADIUS server, you must identify the user profile name.
server *ip-address*	(Optional) For RADIUS server load balancing, specifies to which server in the server group the test packets will be sent.
auth-port	(Optional) User Datagram Protocol (UDP) destination port for authentication requests.

port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1646.
acct-port	(Optional) UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
count *requests*	(Optional) Number of authentication and accounting requests that are to be sent to the server for each port. Range: 1 to 50000. Default: 1.
rate *requests-per-second*	(Optional) Number of requests per second that are to be sent to the server. Range: 1 to 1000. Default: 10.
blocked {**yes** | **no**}	(Optional) Specifies whether the request is sent in blocking or nonblocking mode. If the **blocked** keyword is not used and one request is sent, the default is **yes**; if more than one request is sent, the default is **no**.

Command Default

DNIS or CLID attribute values are not sent to the RADIUS server.

RADIUS Server Load Balancing Manual Testing

RADIUS server load-balancing server status manual testing does not occur.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	The following keywords and arguments were added for configuring RADIUS load balancing manual testing functionality: **server** *ip-address*, **auth-port** *port-number*, **acct-port** *port-number*, **count** *request*, **rate** *requests-per-second*, **blocked**.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)ZV1	This command was enhanced to show user attributes returned from RADIUS authentication when authentication is successful.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

The **test aaa group** command can be used to

- Associate a DNIS or CLID named user profile with the record that is sent to the RADIUS server, which can then access DNIS or CLID information when the server receives a RADIUS record.
- Verify RADIUS load-balancing server status.

Note The **test aaa group**command does not work with TACACS+.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named prfl1 and associate it with a **test aaa group**command:

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

The following example shows the response from a load-balanced RADIUS server that is alive when the username "test" does not match a user profile. The server is verified alive when it issues an Access-Reject response to a AAA packet generated by the **test aaa group** command.

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication ]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

Examples

The following example shows the user attribute list that the RADIUS server returns when you issue the test aaa command and authentication is successful:

```
Router# test aaa group radius viral viral new-code blocked no
AAA/SG/TEST: Sending 1 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
CLI-1#
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Authen Requests to Send    : 1
AAA/SG/TEST:      Authen Requests Processed  : 1
AAA/SG/TEST:      Authen Requests Sent       : 1
AAA/SG/TEST:      Authen Requests Replied    : 1
AAA/SG/TEST:      Authen Requests Successful : 1
AAA/SG/TEST:      Authen Requests Failed     : 0
AAA/SG/TEST:      Authen Requests Error      : 0
AAA/SG/TEST:      Authen Response Received   : 1
AAA/SG/TEST:      Authen No Response Received: 0
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Account Requests to Send    : 0
AAA/SG/TEST:      Account Requests Processed  : 0
AAA/SG/TEST:      Account Requests Sent       : 0
AAA/SG/TEST:      Account Requests Replied    : 0
AAA/SG/TEST:      Account Requests Successful : 0
AAA/SG/TEST:      Account Requests Failed     : 0
AAA/SG/TEST:      Account Requests Error      : 0
AAA/SG/TEST:      Account Response Received   : 0
AAA/SG/TEST:      Account No Response Received: 0
USER ATTRIBUTES
username             "Username:viral"
nas-ip-address       3.1.1.1
interface            "210"
service-type         1 [Login]
Framed-Protocol      3 [ARAP]
ssg-account-info     "S20.5.0.2"
ssg-command-code     0B 4C 32 54 50 53 55 52 46
Router
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
aaa user profile	Creates a AAA user profile.
load-balance	Enables RADIUS server load-balancing for RADIUS-named server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load-balancing for the global RADIUS server group.

timeout (TACACS+)

To configure the time to wait for a reply from the specified TACACS server, use the **timeout**command in TACACS+ server configuration mode. To return to the command default, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	(Optional) Amount of time, in seconds.

Command Default

Time to wait is 5 seconds.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **timeout** command to set the time, in seconds, to wait for a reply from the TACACS server. If the **timeout** command is configured, the specified number of seconds overrides the default time of 5 seconds.

Examples

The following example shows how to configure the wait time to 10 seconds:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS server configuration mode.