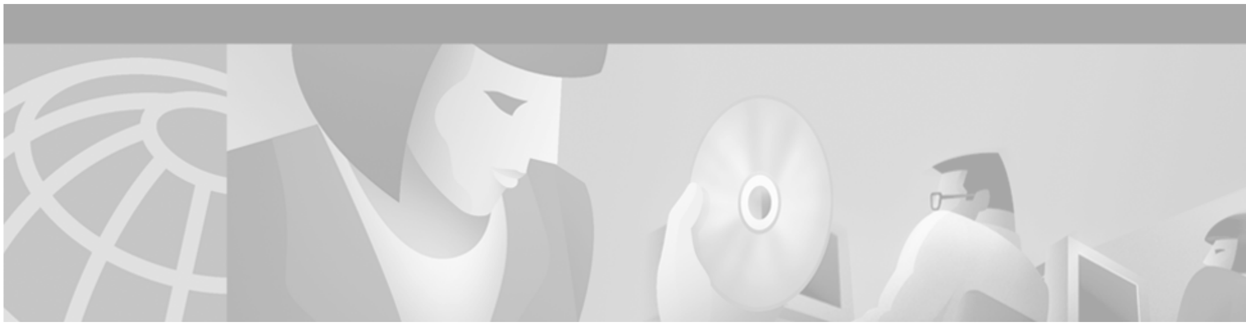

TACACS+ Commands

This chapter describes the commands used to configure TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.

Note Refer to the chapter “Authentication Commands”, the chapter “Authorization Commands”, and the chapter “Accounting Commands” for information about commands specific to AAA.

For information on how to configure TACACS+, refer to the chapter “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the section “TACACS+ Configuration Examples” located at the end of the chapter “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*.

Note TACACS and Extended TACACS commands are included in Cisco IOS Release 12.2 software for backward compatibility with earlier Cisco IOS releases; however, these commands are no longer supported and are not documented for this release.

Cisco recommends using only the TACACS+ security protocol with Release 12.1 and later of Cisco IOS software. For a description of TACACS and Extended TACACS commands, refer to the chapter “TACACS, Extended TACACS, and TACACS+ Commands” in Cisco IOS Release 12.0 *Security Command Reference* at Cisco.com.

Table 17 identifies Cisco IOS software commands available to the different versions of TACACS. Although TACACS+ is enabled through AAA and uses commands specific to AAA, there are some commands that are common to TACACS, Extended TACACS, and TACACS+. TACACS and Extended TACACS commands that are not common to TACACS+ are not documented in this release.

Table 17 TACACS Command Comparison

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
aaa accounting[1]	–	–	yes
aaa authentication arap[1]	–	–	yes
aaa authentication enable default[1]	–	–	yes
aaa authentication login[1]	–	–	yes
aaa authentication ppp[1]	–	–	yes

Table 17 TACACS Command Comparison (continued)

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
aaa authorization[1]	–	–	yes
aaa group server tacacs+			yes
aaa new-model[1]	–	–	yes
arap authentication[1]	–	–	yes
arap use-tacacs	yes	yes	–
enable last-resort	yes	yes	–
enable use-tacacs	yes	yes	–
ip tacacs source-interface	yes	yes	yes
login authentication[1]	–	–	yes
login tacacs	yes	yes	–
ppp authentication[1]	yes	yes	yes
ppp use-tacacs[1]	yes	yes	no
server	–	–	yes
tacacs-server administration	–	–	yes
tacacs-server directed-request	yes	yes	yes
tacacs-server dns-alias-lookup	–	–	yes
tacacs-server host	yes	yes	yes
tacacs-server key	–	–	yes
tacacs-server packet	–	–	yes
tacacs-server timeout	yes	yes	yes

[1] These commands are documented in separate chapters. Refer to the appropriate authentication, authorization, or accounting section of the *Cisco IOS Security Command Reference*, or use the index to locate a command.

aaa group server tacacs+

To group different server hosts into distinct lists and distinct methods, use the **aaa group server tacacs+** command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Syntax Description

tacacs+	Uses only the TACACS+ server hosts.
group-name	Character string used to name the group of servers.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

Examples

The following example shows the configuration of an AAA group server named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
    server 1.1.1.1
    server 2.2.2.2
    server 3.3.3.3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security.
aaa authentication login	Enables AAA accounting of requested services for billing or security purposes.
aaa authorization	Sets parameters that restrict user access to a network.

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Syntax Description

subinterface-name	Name of the interface that TACACS+ uses for all of its outgoing packets.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to set a subinterface's IP address for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a *down* state, TACACS+ reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the *up* state.

Examples

The following example makes TACACS+ use the IP address of subinterface s2 for all outgoing TACACS+ packets:

```
ip tacacs source-interface s2
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

server *ip-address*

no server *ip-address*

Syntax Description

ip-address	IP address of the selected server.

Defaults

No default behavior or values.

Command Modes

TACACS+ group server configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server** command to specify the IP address of the TACACS+ server. Also configure a matching **tacacs-server host** entry in the global list. If there is no response from the first host entry, the next host entry is tried.

Examples

The following example shows server host entries configured for the RADIUS server:

```
aaa new-model
aaa authentication ppp default group g1
aaa group server tacacs+ g1
    server 1.0.0.1
    server 2.0.0.1
tacacs-server host 1.0.0.1
tacacs-server host 2.0.0.1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa server group	Groups different server hosts into distinct lists and distinct methods.
tacacs-server host	Specifies a RADIUS server host.

show tacacs

To display statistics for a TACACS+ server, use the **show tacacs** command in EXEC configuration mode.

show tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following example is sample output for the **show tacacs** command:

```
Router# show tacacs

Tacacs+ Server            : 172.19.192.80/49
              Socket opens:          3
             Socket closes:          3
             Socket aborts:          0
             Socket errors:          0
           Socket Timeouts:          0
   Failed Connect Attempts:          0
        Total Packets Sent:          7
        Total Packets Recv:          7
          Expected Replies:          0
  No current connection
```

Table 18 describes the significant fields shown in the display.

Table 18 show tacacs Field Descriptions

Field	Description
Tacacs+ Server	IP address of the TACACS+ server.
Socket opens	Number of successful TCP socket connections to the TACACS+ server.
Socket closes	Number of successfully closed TCP socket attempts.
Socket aborts	Number of premature TCP socket closures to the TACACS+ server; that is, the peer did not wait for a reply from the server after a the peer sent its request.
Socket errors	Any other socket read or write errors, such as incorrect packet format and length.

Table 18 show tacacs Field Descriptions (continued)

Field	Description
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server.
Total Packets Sent	Number of packets sent to the TACACS+ server.
Total Packets Recv	Number of packets received from the TACACS+ server.
Expected replies	Number of outstanding replies from the TACACS+ server.

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

tacacs-server administration

To enable the handling of administrative messages by the TACACS+ daemon, use the **tacacs-server administration** command in global configuration mode. To disable the handling of administrative messages by the TACACS+ daemon, use the **no** form of this command.

tacacs-server administration

no tacacs-server administration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.

Examples

The following example shows that the TACACS+ daemon is enabled to handle administrative messages:

```
tacacs-server administration
```

tacacs-server directed-request

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request** command in global configuration mode. To send the entire string to the TACACS+ server, use the **no** form of this command.

tacacs-server directed-request [**restricted**] [**no-truncate**]

no tacacs-server directed-request

Syntax Description

restricted	(Optional) Restrict queries to directed request servers only.
no-truncate	(Optional) Do not truncate the @hostname from the username.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling **tacacs-server directed-request** causes the whole string, both before and after the "@" symbol, to be sent to the default TACACS+ server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list, sending the whole string, and accepting the first response that it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS+ server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS+ servers can be specified by the user after the "@" symbol. If the host name specified by the user does not match the IP address of a TACACS+ server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS+ servers and to cause the entire string to be passed to the default server.

Examples

The following example disables **tacacs-server directed-request** so that the entire user input is passed to the default TACACS+ server:

```
no tacacs-server directed-request
```

tacacs-server dns-alias-lookup

To enable IP Domain Name System (DNS) alias lookup for TACACS+ servers, use the command in global configuration mode. To disable IP DNS alias lookup, use the **no** form of this command.

tacacs-server dns-alias-lookup

no tacacs-server dns-alias-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

IP DNS alias lookup is disabled.

Command Modes

global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.

Examples

The following example shows that IP DNS alias lookup has been enabled:

```
tacacs-server dns-alias-lookup
```

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* [**port** *integer*] [**timeout** *integer*] [**key** *string*] [**single-connection**] [**nat**]

no tacacs-server host *host-name*

Syntax Description

host-name	Name or IP address of the host.
port	(Optional) Specifies a 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 to 65535.
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.
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.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
nat	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.

Defaults

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.

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.
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.

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the **tacacs-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

tacacs-server key *key*

no tacacs-server key [*key*]

Syntax Description

key	Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) with the **aaa new-model** command, you must set the authentication and encryption key using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
tacacs-server key dare to go
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

tacacs-server packet

To modify TACACS+ packet options, use the **tacacs-server packet** command in global configuration mode. To disable the modified packet options, use the **no** form of this command.

tacacs-server packet *maxsize*

no tacacs-server packet

Syntax Description

maxsize	Maximum TACACS+ packet size that is acceptable. The value is from 10240 through 65536.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.

Examples

The following example shows that the TACACS+ packet size has been set to the minimum value of 10240:

```
tacacs-server packet 10240
```

tacacs-server timeout

To set the interval for which the server waits for a server host to reply, use the **tacacs-server timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Timeout interval in seconds. The value is from 1 through 1000. The default is 5.

Command Default

If the command is not configured, the timeout interval is 5.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example changes the interval timeout to 10 seconds:

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