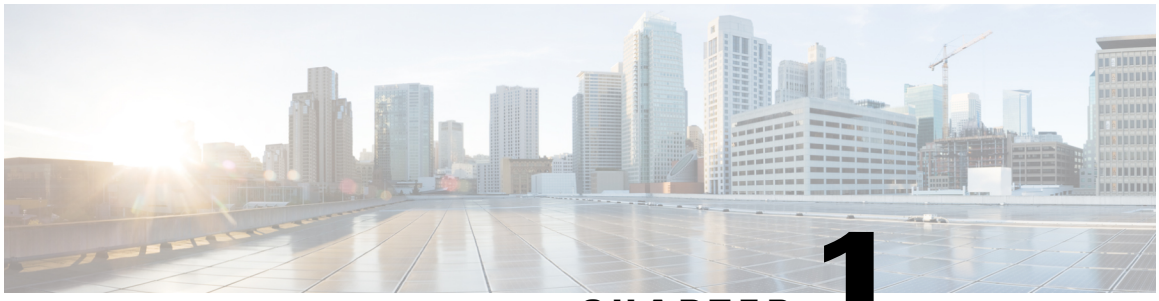
TACACS+ Configuration Guide, Cisco IOS Release 15S

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Configuring TACACS

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring TACACS

You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

Restrictions for Configuring TACACS

TACACS+ can be enabled only through AAA commands.

TACACS Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a device or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation.

TACACS+ provides for separate and modular 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 goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. The Cisco family of access servers and devices and the Cisco IOS user interface (for both devices and access servers) can be network access servers.

Network access points enable traditional “dumb” terminals, terminal emulators, workstations, personal computers (PCs), and devices in conjunction with suitable adapters (for example, modems or ISDN adapters) to communicate using protocols such as Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Compressed SLIP (CSLIP), or AppleTalk Remote Access (ARA) protocol. In other words, a network access server provides connections to a single user, to a network or subnetwork, and to interconnected networks. The entities connected to the network through a network access server are called network access clients; for example, a PC running PPP over a voice-grade circuit is a network access client. TACACS+, administered through the AAA security services, can provide the following services:

- Authentication--Provides complete control of authentication through login and password dialog, challenge and response, messaging support.

The authentication facility provides the ability to conduct an arbitrary dialog with the user (for example, after a login and password are provided, to challenge a user with a number of questions, such as home address, mother’s maiden name, service type, and social security number). In addition, the TACACS+ authentication service supports sending messages to user screens. For example, a message could notify users that their passwords must be changed because of the company’s password aging policy.

- Authorization--Provides fine-grained control over user capabilities for the duration of the user’s session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user may execute with the TACACS+ authorization feature.
- Accounting--Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the network access server and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between a network access server and a TACACS+ daemon are encrypted.

You need a system running TACACS+ daemon software to use the TACACS+ functionality on your network access server.

Cisco makes the TACACS+ protocol specification available as a draft RFC for those customers interested in developing their own TACACS+ software.

TACACS Operation

When a user attempts a simple ASCII login by authenticating to a network access server using TACACS+, the following process typically occurs:

1. When the connection is established, the network access server will contact the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username and the network access server then contacts the TACACS+ daemon to obtain a password prompt. The network access server displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

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

1. The network access server will eventually receive one of the following responses from the TACACS+ daemon:
    1. ACCEPT--The user is authenticated and service may begin. If the network access server is configured to requite authorization, authorization will begin at this time.
    2. REJECT--The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending on the TACACS+ daemon.
    3. ERROR--An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the network access server. If an ERROR response is received, the network access server will typically try to use an alternative method for authenticating the user.
    4. CONTINUE--The user is prompted for additional authentication information.
2. A PAP login is similar to an ASCII login, except that the username and password arrive at the network access server in a PAP protocol packet instead of being typed in by the user, so the user is not prompted. PPP CHAP logins are also similar in principle.

Following authentication, the user will also be required to undergo an additional authorization phase, if authorization has been enabled on the network access server. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

1. If TACACS+ authorization is required, the TACACS+ daemon is again contacted and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response will contain data in the form of attributes that are used to direct the EXEC or NETWORK session for that user, determining services that the user can access. Services include the following:
    1. Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
    2. Connection parameters, including the host or client IP address, access list, and user timeouts

TACACS AV Pairs

The network access server implements TACACS+ authorization and accounting functions by transmitting and receiving TACACS+ attribute-value (AV) pairs for each user session. For a list of supported TACACS+ AV pairs, refer to the appendix "TACACS+ Attribute-Value Pairs."

How to Configure TACACS

To configure your router to support TACACS+, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use TACACS+.
- Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication. See the Configuring Authentication feature module for more information.
- Use **line** and **interface** commands to apply the defined method lists to various interfaces. See the Configuring Authentication feature module for more information.
- If needed, use the **aaa authorization** global command to configure authorization for the network access server. Unlike authentication, which can be configured per line or per interface, authorization is configured globally for the entire network access server. See the Configuring Authorization feature module for more information.
- If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections. See the Configuring Accounting feature module for more information.

Identifying the TACACS Server Host

The **tacacs-server host** command enables you to specify the names of the IP host or hosts maintaining a TACACS+ server. Because the TACACS+ software searches for the hosts in the order specified, this feature can be useful for setting up a list of preferred daemons.

Note The **tacacs-server host** command will be deprecated soon. You can use the **server** command instead of the **tacacs-server host** command.

To specify a TACACS+ host, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **tacacs-server host** *hostname* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	Specifies a TACACS+ host.

Using the **tacacs-server host** command, you can also configure the following options:

- Use the **single-connection** keyword to specify single-connection. Rather than have the router open and close a TCP connection to the daemon each time it must communicate, the single-connection option maintains a single open connection between the router and the daemon. This is more efficient because it allows the daemon to handle a higher number of TACACS operations.

Note The daemon must support single-connection mode for this to be effective, otherwise the connection between the network access server and the daemon will lock up or you will receive spurious errors.

- Use the **port** *integer* argument to specify the TCP port number to be used when making connections to the TACACS+ daemon. The default port number is 49.
- Use the **timeout** *integer* argument to specify the period of time (in seconds) the router will wait for a response from the daemon before it times out and declares an error.

Note Specifying the timeout value with the **tacacs-server host** command overrides the default timeout value set with the **tacacs-server timeout** command for this server only.

- Use the **key** *string* argument to specify an encryption key for encrypting and decrypting all traffic between the network access server and the TACACS+ daemon.

Note Specifying the encryption key with the **tacacs-server host** command overrides the default key set by the global configuration **tacacs-server key** command for this server only.

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 TACACS+ connections.

Setting the TACACS Authentication Key

To set the global TACACS+ authentication key and encryption key used to encrypt all exchanges between the network access server and the TACACS+ daemon, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **tacacs-server key** *key*	Sets the encryption key to match that used on the TACACS+ daemon.

Note The same key must be configured on the TACACS+ daemon for encryption to be successful.

Configuring AAA Server Groups

Configuring the router to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. 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.

Server groups can include multiple host entries as long as each entry has a unique IP address. If two different host entries in the server group are configured for the same service--for example, accounting--the second host entry configured acts as fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry for accounting services. (The TACACS+ host entries will be tried in the order in which they are configured.)

To define a server host with a server group name, enter the following commands starting in global configuration mode. The listed server must exist in global configuration mode:

SUMMARY STEPS

1. Router(config)# **tacacs-server host***name* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]
2. Router(config-if)# **aaa group server**{**radius** | **tacacs+**} *group-name*
3. Router(config-sg)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **tacacs-server host***name* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	Specifies and defines the IP address of the server host before configuring the AAA server-group. See Identifying the TACACS Server Host for more information on the **tacacs-server host** command.
Step 2	Router(config-if)# **aaa group server**{**radius** | **tacacs+**} *group-name*	Defines the AAA server-group with a group name. All members of a group must be the same type; that is, RADIUS or TACACS+. This command puts the router in server group subconfiguration mode.
Step 3	Router(config-sg)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]	Associates a particular TACACS+ server with the defined server group. Use the **auth-port** *port-number* option to configure a specific UDP port solely for authentication. Use the **acct-port** *port-number* option to configure a specific UDP port solely for accounting. Repeat this step for each TACACS+ server in the AAA server group. **Note** Each server in the group must be defined previously using the **tacacs-server host** command.

Configuring AAA Server Group Selection Based on DNIS

Cisco software allows you to authenticate users to a particular AAA server group based on the Dialed Number Identification Service (DNIS) number of the session. Any phone line (a regular home phone or a commercial

T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco devices with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different TACACS+ server groups for different customers (that is, different TACACS+ servers for different DNIS numbers). Additionally, using server groups you can specify the same server group for AAA services or a separate server group for each AAA service.

Cisco IOS software provides the flexibility to implement authentication and accounting services in several ways:

- Globally--AAA services are defined using global configuration access list commands and applied in general to all interfaces on a specific network access server.
- Per interface--AAA services are defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server.
- DNIS mapping--You can use DNIS to specify an AAA server to supply AAA services.

Because AAA configuration methods can be configured simultaneously, Cisco has established an order of precedence to determine which server or groups of servers provide AAA services. The order of precedence is as follows:

- Per DNIS--If you configure the network access server to use DNIS to identify which server group provides AAA services, then this method takes precedence over any additional AAA selection method.
- Per interface--If you configure the network access server per interface to use access lists to determine how a server provides AAA services, this method takes precedence over any global configuration AAA access lists.
- Globally--If you configure the network access server by using global AAA access lists to determine how the security server provides AAA services, this method has the lowest precedence.

Note Prior to configuring AAA Server Group Selection Based on DNIS, you must configure the remote security servers associated with each AAA server group. See Identifying the TACACS Server Host and Configuring AAA Server Groups for more information.

To configure the router to select a particular AAA server group based on the DNIS of the server group, configure DNIS mapping. To map a server group with a group name with DNIS number, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **aaa dnis map enable**
2. Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
3. Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)**# aaa dnis map enable**	Enables DNIS mapping.
Step 2	Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
Step 3	Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting.

Specifying TACACS Authentication

After you have identified the TACACS+ daemon and defined an associated TACACS+ encryption key, you must define method lists for TACACS+ authentication. Because TACACS+ authentication is operated via AAA, you need to issue the **aaa authentication** command, specifying TACACS+ as the authentication method. See the Configuring Authentication feature module for more information.

Specifying TACACS Authorization

AAA authorization enables you to set parameters that restrict a user's access to the network. Authorization via TACACS+ may be applied to commands, network connections, and EXEC sessions. Because TACACS+ authorization is facilitated through AAA, you must issue the **aaa authorization** command, specifying TACACS+ as the authorization method. See the Configuring Authorization feature module for more information.

Specifying TACACS Accounting

AAA accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because TACACS+ accounting is facilitated through AAA, you must issue the **aaa accounting** command, specifying TACACS+ as the accounting method. See the Configuring Accounting feature module for more information.

TACACS Configuration Examples

TACACS Authentication Examples

The following example shows how to configure TACACS+ as the security protocol for PPP authentication:

```
aaa new-model
```

```
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap pap test
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, "test," to be used on serial interfaces running PPP. The keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be "goaway."
- The **interface** command selects the line, and the **ppp authentication** command applies the test method list to this line.

The following example shows how to configure TACACS+ as the security protocol for PPP authentication, but instead of the "test" method list, the "default" method list is used.

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, "default," to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be "goaway."
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The following example shows how to create the same authentication algorithm for PAP, but it calls the method list "MIS-access" instead of "default":

```
aaa new-model
aaa authentication pap MIS-access if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication pap MIS-access
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.

- The **aaa authentication** command defines a method list, “MIS-access,” to be used on serial interfaces running PPP. The method list, “MIS-access,” means that PPP authentication is applied to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The following example shows the configuration for a TACACS+ daemon with an IP address of 10.2.3.4 and an encryption key of “apple”:

```
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.2.3.4
tacacs-server key apple
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines the default method list. Incoming ASCII logins on all interfaces (by default) will use TACACS+ for authentication. If no TACACS+ server responds, then the network access server will use the information contained in the local username database for authentication.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.2.3.4. The **tacacs-server key** command defines the shared encryption key to be “apple.”

TACACS Authorization Example

The following example shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure network authorization via TACACS+:

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

- The **aaa authorization** command configures network authorization via TACACS+. Unlike authentication lists, this authorization list always applies to all incoming network connections made to the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

TACACS Accounting Example

The following example shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure accounting via TACACS+:

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **aaa accounting** command configures network accounting via TACACS+. In this example, accounting records describing the session that just terminated will be sent to the TACACS+ daemon whenever a network connection terminates.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

TACACS Server Group Example

The following example shows how to create a server group with three different TACACS+ servers members:

```
aaa group server tacacs tacgroup1
server 172.16.1.1
server 172.16.1.21
server 172.16.1.31
```

AAA Server Group Selection Based on DNIS Example

The following example shows how to select TACAC+ server groups based on DNIS to provide specific AAA services:

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the TACACS+ servers that will be associated
! with one of the defined server groups.
tacacs-server host 172.16.0.1
tacacs-server host 172.17.0.1
tacacs-server host 172.18.0.1
tacacs-server host 172.19.0.1
tacacs-server host 172.20.0.1
tacacs-server key abcdefg
! The following commands define the sg1 TACACS+ server group and associate servers
! with it.
aaa group server tacacs sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg2
  server 172.18.0.1
! The following commands define the sg3 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg3
  server 172.19.0.1
! The following commands define the default-group TACACS+ server group and associate
! a server with it.
aaa group server tacacs default-group
  server 172.20.0.1
!
! The next set of commands configures default-group tacacs server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using DNIS
! 7777 are sent to the sg1 server group. The accounting records for these connections
! (specifically, start-stop records) are handled by the sg2 server group. Calls with a
! DNIS of 8888 use server group sg3 for authentication and server group default-group
! for accounting. Calls with a DNIS of 9999 use server group default-group for
! authentication and server group sg3 for accounting records (stop records only). All
! other calls with DNIS other than the ones defined use the server group default-group
! for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

TACACS Daemon Configuration Example

The following example shows a sample configuration of the TACACS+ daemon. The precise syntax used by your TACACS+ daemon may be different from what is included in this example.

```
user = mci_customer1 {
 chap = cleartext “some chap password”
 service = ppp protocol = ip {
inacl#1=”permit ip any any precedence immediate”
inacl#2=”deny igrp 0.0.1.2 255.255.0.0 any”
 }
```

Additional References

The following sections provide references related to the Configuring TACACS+ feature.

Related Documents

Related Topic	Document Title
AAA	Cisco IOS Security Guide: Securing User Services

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring TACACS

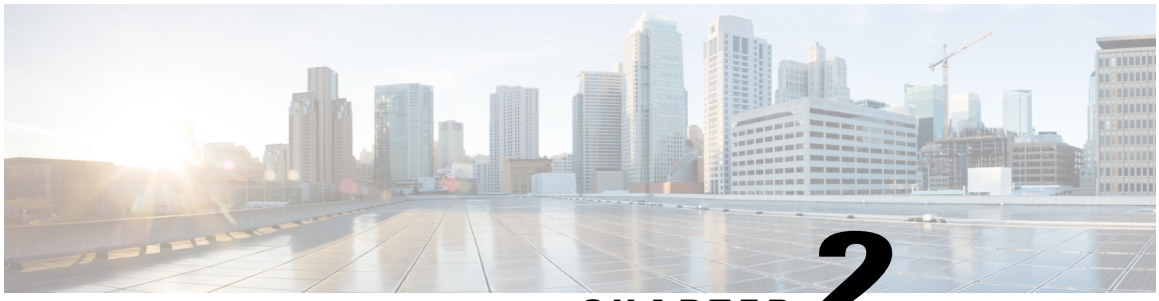
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring TACACS+

Feature Name	Releases	Feature Information
Configuring TACACS+		TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands. The following commands were introduced or modified: **tacacs-server host**, **tacacs-server key**, **aaa authentication**, **aaa accounting**, **aaa group server tacacs+**.

Feature Name	Releases	Feature Information
AAA Server Groups Based on DNIS		The AAA Server Groups Based on DNIS feature allows you to authenticate users to a particular AAA server group based on the Dialed Number Identification Service (DNIS) number of the session. The following commands were introduced or modified: **aaa dnis map enable**, **aaa dnis map authentication group**, **aaa dnis map accounting**.



CHAPTER 2

Per VRF for TACACS Servers

The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Per VRF for TACACS Servers

- TACACS+ server access is required.
- Experience configuring TACACS+, AAA and per VRF AAA, and group servers is necessary.

Restrictions for Per VRF for TACACS Servers

- The VRF instance must be specified before per VRF for a TACACS+ server is configured.

Information About Per VRF for TACACS Servers

Per VRF for TACACS Servers Overview

The Per VRF for TACACS+ Servers feature allows per VRF AAA to be configured on TACACS+ servers. Prior to Cisco IOS Release 12.3(7)T, this functionality was available only on RADIUS servers.

How to Configure Per VRF for TACACS Servers

Configuring Per VRF on a TACACS Server

The initial steps in this procedure are used to configure AAA and a server group, create a VRF routing table, and configure an interface. Steps 10 through 13 are used to configure the per VRF on a TACACS+ server feature:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **interface** *interface-name*
7. **ip vrf forwarding** *vrf-name*
8. **ip address** *ip-address mask* [**secondary**]
9. **exit**
10. **aaa group server tacacs+** *group-name*
11. **server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]
12. **ip vrf forwarding** *vrf-name*
13. **ip tacacs source-interface** *subinterface-name*
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Router (config)# ip vrf cisco`	Configures a VRF table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Router (config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF instance.
Step 5	**exit** **Example:** `Router (config-vrf)# exit`	Exits VRF configuration mode.
Step 6	**interface** *interface-name* **Example:** `Router (config)# interface Loopback0`	Configures an interface and enters interface configuration mode.
Step 7	**ip vrf forwarding** *vrf-name* **Example:** `Router (config-if)# ip vrf forwarding cisco`	Configures a VRF for the interface.
Step 8	**ip address** *ip-address mask* [**secondary**] **Example:** `Router (config-if)# ip address 10.0.0.2 255.0.0.0`	Sets a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router (config-if)# exit`	Exits interface configuration mode.
Step 10	**aaa group server tacacs+** *group-name* **Example:** `Router (config)# aaa group server tacacs+ tacacs1`	Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 11	**server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] **Example:** `Router (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco`	Configures the IP address of the private TACACS+ server for the group server.
Step 12	**ip vrf forwarding** *vrf-name* **Example:** `Router (config-sg-tacacs+)# ip vrf forwarding cisco`	Configures the VRF reference of a AAA TACACS+ server group.
Step 13	**ip tacacs source-interface** *subinterface-name* **Example:** `Router (config-sg-tacacs+)# ip tacacs source-interface Loopback0`	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
Step 14	**exit** **Example:** `Router (config-sg-tacacs)# exit`	Exits server-group configuration mode.

Verifying Per VRF for TACACS Servers

To verify the per VRF TACACS+ configuration, perform the following steps:

Note The **debug** commands may be used in any order.

SUMMARY STEPS

1. enable
2. debug tacacs authentication
3. debug tacacs authorization
4. debug tacacs accounting
5. debug tacacs packets

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug tacacs authentication** **Example:** `Router# debug tacacs authentication`	Displays information about AAA/TACACS+ authentication.
Step 3	**debug tacacs authorization** **Example:** `Router# debug tacacs authorization`	Displays information about AAA/TACACS+ authorization.
Step 4	**debug tacacs accounting** **Example:** `Router# debug tacacs accounting`	Displays information about accountable events as they occur.
Step 5	**debug tacacs packets** **Example:** `Router# debug tacacs packets`	Displays information about TACACS+ packets.

Configuration Examples for Per VRF for TACACS Servers

Configuring Per VRF for TACACS Servers Example

The following output example shows that the group server **tacacs1** is configured for per VRF AAA services:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0
  ip vrf cisco
   rd 100:1
  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Additional References

The following sections provide references related to Per VRF for TACACS+ Servers..

Related Documents

Related Topic	Document Title
Configuring TACACS+	Configuring TACACS+ module.
Per VRF AAA	Per VRF AAA module.
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Per VRF for TACACS Servers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Per VRF for TACACS+ Servers

Feature Name	Releases	Feature Information
Per VRF for TACACS+ Servers	12.3(7)T 12.2(33)SRA1 12.2(33)SXI 12.2(33)SXH4 12.2(54)SG 15.2(1)E	The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers. This feature was introduced in Cisco IOS Release 12.3(7)T. This feature was integrated into Cisco IOS Release 12.2(33)SRA1. This feature was integrated into Cisco IOS Release 12.2(33)SXI. This feature was integrated into Cisco IOS Release 12.2(33)SXH4. The following commands were introduced or modified: **ip tacacs source-interface**, **ip vrf forwarding (server-group)**, **server-private (TACACS+)**.