



## **TACACS+ Configuration Guide Cisco IOS XE Release 2**

### **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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### Configuring TACACS 1

- Finding Feature Information 1
- Information About TACACS 1
  - TACACS Operation 2
- How to Configure TACACS 3
  - Identifying the TACACS Server Host 4
  - Setting the TACACS Authentication Key 5
  - Configuring AAA Server Groups 5
  - Configuring AAA Server Group Selection Based on DNIS 6
  - Specifying TACACS Authentication 7
  - Specifying TACACS Authorization 7
  - Specifying TACACS Accounting 8
  - TACACS AV Pairs 8
- TACACS Configuration Examples 8
  - TACACS Authentication Examples 8
  - TACACS Authorization Example 10
  - TACACS Accounting Example 10
  - TACACS Server Group Example 11
  - AAA Server Group Selection Based on DNIS Example 11
  - TACACS Daemon Configuration Example 12
- Additional References 12
- Feature Information for Configuring TACACS 13

### Per VRF for TACACS Servers 15

- Finding Feature Information 15
- Prerequisites for Per VRF for TACACS Servers 15
- Restrictions for Per VRF for TACACS Servers 15
- Information About Per VRF for TACACS Servers 16
  - Per VRF for TACACS Servers Overview 16
- How to Configure Per VRF for TACACS Servers 16

Configuring Per VRF on a TACACS Server	16
Verifying Per VRF for TACACS Servers	19
Configuration Examples for Per VRF for TACACS Servers	20
Configuring Per VRF for TACACS Servers Example	20
Additional References	20
Feature Information for Per VRF for TACACS Servers	21
<b>TACACS Attribute-Value Pairs</b>	<b>23</b>
Information About TACACS Attribute-Value Pairs	23
TACACS Authentication and Authorization AV Pairs	23
TACACS Accounting AV Pairs	36



# Configuring TACACS

---

This chapter discusses how to enable and configure TACACS+, which 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, page 1](#)
- [Information About TACACS, page 1](#)
- [How to Configure TACACS, page 3](#)
- [TACACS Configuration Examples, page 8](#)
- [Additional References, page 12](#)
- [Feature Information for Configuring TACACS, page 13](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Information About TACACS

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

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 routers and the Cisco IOS and Cisco IOS XE user interface (for both routers and access servers) can be network access servers.

Network access points enable traditional “dumb” terminals, terminal emulators, workstations, personal computers (PCs), and routers 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, like 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, page 2](#)

## 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:
  - a ACCEPT--The user is authenticated and service may begin. If the network access server is configured to require authorization, authorization will begin at this time.
  - b 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.
  - c 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.
  - d 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:
  - a Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
  - b Connection parameters, including the host or client IP address, access list, and user timeouts

## 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+. For more information about using the **aaa new-model** command, refer to the chapter “AAA Overview”.
- Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons. Use the **tacacs-server key** command to specify an encryption key that will be used to encrypt all exchanges between the network access server and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon.
- Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication. For more information about using the **aaa authentication** command, refer to the chapter “Configuring Authentication”.
- Use line and interface commands to apply the defined method lists to various interfaces. For more information, refer to the chapter “Configuring Authentication”.
- 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. For more information about using the **aaa authorization** command, refer to the “Configuring Authorization” chapter.

- If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections. For more information about using the **aaa accounting** command, refer to the “Configuring Accounting” chapter.
- [Identifying the TACACS Server Host, page 4](#)
- [Setting the TACACS Authentication Key, page 5](#)
- [Configuring AAA Server Groups, page 5](#)
- [Configuring AAA Server Group Selection Based on DNIS, page 6](#)
- [Specifying TACACS Authentication, page 7](#)
- [Specifying TACACS Authorization, page 7](#)
- [Specifying TACACS Accounting, page 8](#)
- [TACACS AV Pairs, page 8](#)

## 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)# <b>tacacs-server host</b> <i>hostname</i> [ <b>single-connection</b> ] [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <i>string</i> ]	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 (only valid with CiscoSecure Release 1.0.1 or later). 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, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>tacacs-server key</b> <i>key</i>	Sets the encryption key to match that used on the TACACS+ daemon.

**Note**

You must configure the same key 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
<b>Step 1</b>	Router(config)# <b>tacacs-server</b> <i>host name</i> [ <b>single-connection</b> ] [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <i>string</i> ]	Specifies and defines the IP address of the server host before configuring the AAA server-group. Refer to the Identifying the TACACS Server Host section of this chapter for more information on the <b>tacacs-server host</b> command.
<b>Step 2</b>	Router(config-if)# <b>aaa group server</b> { <b>radius</b>   <b>tacacs+</b> } <i>group-name</i>	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.
<b>Step 3</b>	Router(config-sg)# <b>server</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ] [ <b>acct-port</b> <i>port-number</i> ]	<p>Associates a particular TACACS+ server with the defined server group. Use the <b>auth-port</b> <i>port-number</i> option to configure a specific UDP port solely for authentication. Use the <b>acct-port</b> <i>port-number</i> option to configure a specific UDP port solely for accounting.</p> <p>Repeat this step for each TACACS+ server in the AAA server group.</p> <p><b>Note</b> Each server in the group must be defined previously using the <b>tacacs-server host</b> command.</p>

**Configuring AAA Server Group Selection Based on DNIS**

Cisco IOS XE 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 routers 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 XE 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 the Identifying the TACACS Server Host and Configuring AAA Server Groups.

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
<b>Step 1</b>	Router(config)# <b>aaa dnis map enable</b>	Enables DNIS mapping.
<b>Step 2</b>	Router(config)# <b>aaa dnis map dnis-number authentication ppp group server-group-name</b>	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
<b>Step 3</b>	Router(config)# <b>aaa dnis map dnis-number accounting network [none   start-stop   stop-only] group server-group-name</b>	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. For more information, refer to the chapter “Configuring Authentication.”

## 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. For more information, refer to the chapter “Configuring Authorization.”

## 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. For more information, refer to the chapter “Configuring Accounting.”

## 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 TACACS Attribute-Value Pairs chapter.

## TACACS Configuration Examples

- [TACACS Authentication Examples, page 8](#)
- [TACACS Authorization Example, page 10](#)
- [TACACS Accounting Example, page 10](#)
- [TACACS Server Group Example, page 11](#)
- [AAA Server Group Selection Based on DNIS Example, page 11](#)
- [TACACS Daemon Configuration Example, page 12](#)

## 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 TACACS+ 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 dn timer enable
aaa dn timer map 7777 authentication ppp group sg1
aaa dn timer map 7777 accounting network start-stop group sg2
aaa dn timer map 8888 authentication ppp group sg3
aaa dn timer 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
TACACS+ commands	<i>Cisco IOS Security Command Reference</i>

### 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 XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>



**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.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>
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.	

## 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](http://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
TACACS+	Cisco IOS XE Release 2.1	<p>TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: <b>tacacs-server host</b>, <b>tacacs-server key</b>, <b>aaa authentication</b>, <b>aaa accounting</b>, <b>aaa group server tacacs+</b>.</p>
AAA Server Groups Based on DNIS	Cisco IOS XE Release 2.3	<p>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.</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: <b>aaa dnis map enable</b>, <b>aaa dnis map authentication group</b>, <b>aaa dnis map accounting</b>.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



## 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, page 15](#)
- [Prerequisites for Per VRF for TACACS Servers, page 15](#)
- [Restrictions for Per VRF for TACACS Servers, page 15](#)
- [Information About Per VRF for TACACS Servers, page 16](#)
- [How to Configure Per VRF for TACACS Servers, page 16](#)
- [Configuration Examples for Per VRF for TACACS Servers, page 20](#)
- [Additional References, page 20](#)
- [Feature Information for Per VRF for TACACS Servers, page 21](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://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 enabled globally on the router before per VRF for a TACACS+ server is configured.

# Information About Per VRF for TACACS Servers

- [Per VRF for TACACS Servers Overview, page 16](#)

## 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 XE Release 2.2, this functionality was available only on RADIUS servers.

## How to Configure Per VRF for TACACS Servers

- [Configuring Per VRF on a TACACS Server, page 16](#)
- [Verifying Per VRF for TACACS Servers, page 19](#)

## 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip vrf vrf-name</b>  <b>Example:</b> Router (config)# ip vrf cisco	Configures a VRF table and enters VRF configuration mode.
<b>Step 4</b>	<b>rd route-distinguisher</b>  <b>Example:</b> Router (config-vrf)# rd 100:1	Creates routing and forwarding tables for a VRF instance.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Router (config-vrf)# exit	Exits VRF configuration mode.
<b>Step 6</b>	<b>interface interface-name</b>  <b>Example:</b> Router (config)# interface Loopback0	Configures an interface and enters interface configuration mode.
<b>Step 7</b>	<b>ip vrf forwarding vrf-name</b>  <b>Example:</b> Router (config-if)# ip vrf forwarding cisco	Configures a VRF for the interface.

	Command or Action	Purpose
<b>Step 8</b>	<b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]  <b>Example:</b> Router (config-if)# ip address 10.0.0.2 255.0.0.0	Sets a primary or secondary IP address for an interface.
<b>Step 9</b>	<b>exit</b>  <b>Example:</b> Router (config-if)# exit	Exits interface configuration mode.
<b>Step 10</b>	<b>aaa group server tacacs+</b> <i>group-name</i>  <b>Example:</b> Router (config)# aaa group server tacacs+ tacacs1	Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode.
<b>Step 11</b>	<b>server-private</b> { <i>ip-address   name</i> } [ <b>nat</b> ] [ <b>single-connection</b> ] [ <b>port</b> <i>port-number</i> ] [ <b>timeout</b> <i>seconds</i> ] [ <b>key</b> [ <b>0</b>   <b>7</b> ] <i>string</i> ]  <b>Example:</b> 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.
<b>Step 12</b>	<b>ip vrf forwarding</b> <i>vrf-name</i>  <b>Example:</b> Router (config-sg-tacacs+)# ip vrf forwarding cisco	Configures the VRF reference of a AAA TACACS+ server group.
<b>Step 13</b>	<b>ip tacacs source-interface</b> <i>subinterface-name</i>  <b>Example:</b> Router (config-sg-tacacs+)# ip tacacs source-interface Loopback0	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
<b>Step 14</b>	<b>exit</b>  <b>Example:</b> 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.

**Caution**

Enabling debug CLI can cause performance degradation on the router. Use of **debug** commands for large number of sessions is not recommended.

### 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>debug tacacs authentication</b>  <b>Example:</b> Router# debug tacacs authentication	Displays information about AAA/TACACS+ authentication.
Step 3	<b>debug tacacs authorization</b>  <b>Example:</b> Router# debug tacacs authorization	Displays information about AAA/TACACS+ authorization.
Step 4	<b>debug tacacs accounting</b>  <b>Example:</b> Router# debug tacacs accounting	Displays information about accountable events as they occur.

Command or Action	Purpose
<b>Step 5</b> <b>debug tacacs packets</b>  <b>Example:</b>  Router# debug tacacs packets	Displays information about TACACS+ packets.

## Configuration Examples for Per VRF for TACACS Servers

- [Configuring Per VRF for TACACS Servers Example, page 20](#)

### 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+ chapter of the Security Server Protocols section of the Cisco IOS XE Security Configuration Guide: Securing User Services, Release 2
Per VRF AAA	Per VRF AAA module
Cisco IOS XE commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Security commands	<i>Cisco IOS Security Command Reference</i>



**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 XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>
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.	

## 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](http://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	Cisco IOS XE Release 2.2	<p>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.</p> <p>In Cisco IOS XE Release 2.2, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: <b>ip tacacs source-interface</b>, <b>ip vrf forwarding (server-group)</b>, <b>server-private (TACACS+)</b>.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



# TACACS Attribute-Value Pairs

Terminal Access Controller Access Control System Plus (TACACS+) attribute-value (AV) pairs are used to define specific authentication, authorization, and accounting elements in a user profile that is stored on the TACACS+ daemon. This chapter lists the TACACS+ AV pairs currently supported.

- [Information About TACACS Attribute-Value Pairs, page 23](#)

## Information About TACACS Attribute-Value Pairs

- [TACACS Authentication and Authorization AV Pairs, page 23](#)
- [TACACS Accounting AV Pairs, page 36](#)

## TACACS Authentication and Authorization AV Pairs

The following table lists and describes the supported TACACS+ authentication and authorization AV pairs and specifies the Cisco IOS release in which they are implemented.

**Table 3**      **Supported TACACS+ Authentication and Authorization AV Pairs**

Attribute	Description	IOS XE 2.1
acl=x	ASCII number representing a connection access list. Used only when service=shell.	yes
addr=x	A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=10.2.3.4.	yes

Attribute	Description	IOS XE 2.1
addr-pool=x	<p>Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip.</p> <p>Note that <b>addr-pool</b> works in conjunction with local pooling. It specifies the name of a local pool (which must be preconfigured on the network access server). Use the <b>ip-local pool</b> command to declare local pools. For example:</p> <pre>ip address-pool local ip local pool boo 10.0.0.1 10.0.0.10 ip local pool moo 10.0.0.1 10.0.0.20</pre> <p>You can then use TACACS+ to return addr-pool=boo or addr-pool=moo to indicate the address pool from which you want to get this remote node's address.</p>	yes
autocmd=x	<p>Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet example.com). Used only with service=shell.</p>	yes
callback- dialstring	<p>Sets the telephone number for a callback (for example: callback-dialstring= 408-555-1212). Value is NULL, or a dial-string. A NULL value indicates that the service might choose to get the dial string through other means. Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.</p>	yes
callback-line	<p>The number of a TTY line to use for callback (for example: callback-line=4). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.</p>	yes

Attribute	Description	IOS XE 2.1
callback-rotary	The number of a rotary group (between 0 and 100 inclusive) to use for callback (for example: callback-rotary=34). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.	yes
cmd-arg=x	An argument to a shell (EXEC) command. This indicates an argument for the shell command that is to be run. Multiple cmd-arg attributes can be specified, and they are order dependent.  <b>Note</b> This TACACS+ AV pair cannot be used with RADIUS attribute 26.	yes
cmd=x	A shell (EXEC) command. This indicates the command name for a shell command that is to be run. This attribute must be specified if service equals "shell." A NULL value indicates that the shell itself is being referred to.  <b>Note</b> This TACACS+ AV pair cannot be used with RADIUS attribute 26.	yes
data-service	Used with the service=outbound and protocol=ip.	yes
dial-number	Defines the number to dial. Used with the service=outbound and protocol=ip.	yes
dns-servers=	Identifies a DNS server (primary or secondary) that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each DNS server is entered in dotted decimal format.	yes

Attribute	Description	IOS XE 2.1
force-56	Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available. To turn on this attribute, use the “true” value (force-56=true). Any other value is treated as false. Used with the service=outbound and protocol=ip.	yes
gw-password	Specifies the password for the home gateway during the L2TP tunnel authentication. Used with service=ppp and protocol=vpdn.	yes
idletime=x	Sets a value, in minutes, after which an idle session is terminated. A value of zero indicates no timeout.	yes
inac1#<n>	ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.	yes
inac1=x	ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Per-user access lists do not currently work with ISDN interfaces.	yes

Attribute	Description	IOS XE 2.1
interface-config#<n>	<p>Specifies user-specific AAA interface configuration information with Virtual Profiles. The information that follows the equal sign (=) can be any Cisco IOS interface configuration command. Multiple instances of the attributes are allowed, but each instance must have a unique number. Used with service=ppp and protocol=lcp.</p> <p><b>Note</b> This attribute replaces the “interface-config=” attribute.</p>	yes
ip-addresses	Space-separated list of possible IP addresses that can be used for the end-point of a tunnel. Used with service=ppp and protocol=vpdn.	yes
l2tp-busy- disconnect	<p>If a vpdn-group on an LNS uses a virtual-template that is configured to be pre-cloned, this attribute will control the disposition of a new L2TP session that finds no pre-cloned interface to which to connect. If the attribute is true (the default), the session will be disconnected by the LNS. Otherwise, a new interface will be cloned from the virtual-template. Used with service=ppp and protocol=vpdn.</p>	yes
l2tp-cm-local- window-size	Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment. Used with service=ppp and protocol=vpdn.	yes

Attribute	Description	IOS XE 2.1
l2tp-drop-out-of- order	Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received. Used with service=ppp and protocol=vpdn.	yes
l2tp-hello- interval	Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here. Used with service=ppp and protocol=vpdn.	yes
l2tp-hidden-avp	When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden. Used with service=ppp and protocol=vpdn.	yes
l2tp-nosession- timeout	Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down. Used with service=ppp and protocol=vpdn.	yes
l2tp-tos-reflect	Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS. Used with service=ppp and protocol=vpdn.	yes
l2tp-tunnel- authen	If this attribute is set, it performs L2TP tunnel authentication. Used with service=ppp and protocol=vpdn.	yes
l2tp-tunnel- password	Shared secret used for L2TP tunnel authentication and AVP hiding. Used with service=ppp and protocol=vpdn.	yes



Attribute	Description	IOS XE 2.1
l2tp-udp- checksum	This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no. Used with service=ppp and protocol=vpdn.	yes
link- compression=	<p>Defines whether to turn on or turn off “stac” compression over a PPP link. Used with service=ppp.</p> <p>Link compression is defined as a numeric value as follows:</p> <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Stac</li> <li>• 2: Stac-Draft-9</li> <li>• 3: MS-Stac</li> </ul>	yes
load-threshold= <n>	Sets the load threshold for the caller at which additional links are either added to or deleted from the multilink bundle. If the load goes above the specified value, additional links are added. If the load goes below the specified value, links are deleted. Used with service=ppp and protocol=multilink. The range for <n> is from 1 to 255.	yes
map-class	Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out. Used with the service=outbound and protocol=ip.	yes
max-links=<n>	Restricts the number of links that a user can have in a multilink bundle. Used with service=ppp and protocol=multilink. The range for <n> is from 1 to 255.	yes
min-links	Sets the minimum number of links for MLP. Used with service=ppp and protocol=multilink, protocol=vpdn.	yes

Attribute	Description	IOS XE 2.1
nas-password	Specifies the password for the network access server during the L2TP tunnel authentication. Used with service=ppp and protocol=vpdn.	yes
nocallback-verify	Indicates that no callback verification is required. The only valid value for this parameter is 1 (for example, nocallback-verify=1). Used with service=arap, service=slip, service=ppp, service=shell. There is no authentication on callback. Not valid for ISDN.	yes
noescape=x	Prevents user from using an escape character. Used with service=shell. Can be either true or false (for example, noescape=true).	yes
nohangup=x	Used with service=shell. Specifies the nohangup option, which means that after an EXEC shell is terminated, the user is presented with another login (username) prompt. Can be either true or false (for example, nohangup=false).	yes
old-prompts	Allows providers to make the prompts in TACACS+ appear identical to those of earlier systems (TACACS and Extended TACACS). This allows administrators to upgrade from TACACS or Extended TACACS to TACACS+ transparently to users.	yes

Attribute	Description	IOS XE 2.1
outacl#<n>	ASCII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current condition. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.	yes
outacl=x	ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be preconfigured on the router. Per-user access lists do not currently work with ISDN interfaces.	yes
pool-def#<n>	Defines IP address pools on the network access server. Used with service=ppp and protocol=ip.	yes
pool-timeout=	Defines (in conjunction with pool-def) IP address pools on the network access server. During IPCP address negotiation, if an IP pool name is specified for a user (see the addr-pool attribute), a check is made to see if the named pool is defined on the network access server. If it is, the pool is consulted for an IP address. Used with service=ppp and protocol=ip.	yes

Attribute	Description	IOS XE 2.1
port-type	<p>Indicates the type of physical port the network access server is using to authenticate the user.</p> <p>Physical ports are indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> <li>0: Asynchronous</li> <li>1: Synchronous</li> <li>2: ISDN-Synchronous</li> <li>3: ISDN-Asynchronous (V. 120)</li> <li>4: ISDN- Asynchronous (V. 110)</li> <li>5: Virtual</li> </ul> <p>Used with service=any and protocol=aaa.</p>	yes
ppp-vj-slot- compression	Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.	yes
priv-lvl=x	Privilege level to be assigned for the EXEC. Used with service=shell. Privilege levels range from 0 to 15, with 15 being the highest.	yes
protocol=x	A protocol that is a subset of a service. An example would be any PPP NCP. Currently known values are <b>lcp, ip, ipx, atalk, vines, lat, xremote, tn3270, telnet, rlogin, pad, vpdn, osicp, deccp, ccp, cdp, bridging, xns, nbff, bap, multilink</b> , and <b>unknown</b> .	yes
proxyacl#<n>	Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces. Used with the service=shell and protocol=exec.	yes

Attribute	Description	IOS XE 2.1
route	<p>Specifies a route to be applied to an interface. Used with service=slip, service=ppp, and protocol=ip.</p> <p>During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows:</p> <pre>route=" dst_address mask [ gateway ]"</pre> <p>This indicates a temporary static route that is to be applied. The <i>dst_address</i> , <i>mask</i> , and <i>gateway</i> are expected to be in the usual dotted-decimal notation, with the same meanings as in the familiar <b>ip route</b> configuration command on a network access server.</p> <p>If <i>gateway</i> is omitted, the peer's address is the gateway. The route is expunged when the connection terminates.</p>	yes
route#<n>	Like the route AV pair, this specifies a route to be applied to an interface, but these routes are numbered, allowing multiple routes to be applied. Used with service=ppp and protocol=ip, and service=ppp and protocol=ipx.	yes
routing=x	<p>Specifies whether routing information is to be propagated to and accepted from this interface. Used with service=slip, service=ppp, and protocol=ip. Equivalent in function to the / routing flag in SLIP and PPP commands. Can either be true or false (for example, routing=true).</p>	yes

Attribute	Description	IOS XE 2.1
rte-fltr-in#<n>	Specifies an input access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.	yes
rte-fltr-out#<n>	Specifies an output access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.	yes
sap#<n>	Specifies static Service Advertising Protocol (SAP) entries to be installed for the duration of a connection. Used with service=ppp and protocol=ipx.	yes
sap-fltr-in#<n>	Specifies an input SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.	yes
sap-fltr-out#<n>	Specifies an output SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.	yes
send-auth	Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication. Used with service=any and protocol=aaa.	yes

Attribute	Description	IOS XE 2.1
send-secret	Specifies the password that the NAS needs to respond to a chap/pap request from the remote end of a connection on an outgoing call. Used with service=ppp and protocol=ip.	yes
service=x	The primary service. Specifying a service attribute indicates that this is a request for authorization or accounting of that service. Current values are <b>slip</b> , <b>ppp</b> , <b>arap</b> , <b>shell</b> , <b>tty-daemon</b> , <b>connection</b> , and <b>system</b> . This attribute must always be included.	yes
source-ip=x	Used as the source IP address of all VPDN packets generated as part of a VPDN tunnel. This is equivalent to the Cisco <b>vpdn outgoing</b> global configuration command.	yes
spi	Carries the authentication information needed by the home agent to authenticate a mobile node during registration. The information is in the same syntax as the <b>ip mobile secure host &lt;addr&gt;</b> configuration command. Basically it contains the rest of the configuration command that follows that string, verbatim. It provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range. Used with the service=mobileip and protocol=ip.	yes
timeout=x	The number of minutes before an EXEC or ARA session disconnects (for example, timeout=60). A value of zero indicates no timeout. Used with service=arap.	yes

Attribute	Description	IOS XE 2.1
tunnel-id	Specifies the username that will be used to authenticate the tunnel over which the individual user MID will be projected. This is analogous to the <i>remote name</i> in the <b>vpdn outgoing</b> command. Used with service=ppp and protocol=vpdn.	yes
wins-servers=	Identifies a Windows NT server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each Windows NT server is entered in dotted decimal format.	yes
zonelist=x	A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5).	yes

For more information about configuring TACACS+, refer to the chapter “Configuring TACACS+.” For more information about configuring TACACS+ authentication and authorization, refer to the chapters “Configuring Authentication” and “Configuring Authorization.”

## TACACS Accounting AV Pairs

The following table lists and describes the supported TACACS+ accounting AV pairs and specifies the Cisco IOS XE release in which they are implemented.

**Table 4**      **Supported TACACS+ Accounting AV Pairs**

Attribute	Description	IOS XE 2.1
Abort-Cause	If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.	yes



Attribute	Description	IOS XE 2.1
bytes_in	The number of input bytes transferred during this connection.	yes
bytes_out	The number of output bytes transferred during this connection.	yes
Call-Type	Describes the type of fax activity: fax receive or fax send.	yes
cmd	The command the user executed.	yes
data-rate	This AV pair has been renamed. See nas-rx-speed.	
disc-cause	Specifies the reason a connection was taken off-line. The Disconnect-Cause attribute is sent in accounting-stop records. This attribute also causes stop records to be generated without first generating start records if disconnection occurs before authentication is performed. Refer to the following table (Disconnect Cause Extensions) for a list of Disconnect-Cause values and their meanings.	yes
disc-cause-ext	Extends the disc-cause attribute to support vendor-specific reasons why a connection was taken off-line.	yes
elapsed_time	The elapsed time in seconds for the action. Useful when the device does not keep real time.	yes
Email-Server- Address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.	yes
Email-Server-Ack- Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.	yes

Attribute	Description	IOS XE 2.1
event	Information included in the accounting packet that describes a state change in the router. Events described are accounting starting and accounting stopping.	yes
Fax-Account-Id- Origin	Indicates the account ID origin as defined by system administrator for the <b>mmoip aaa receive-id</b> or the <b>mmoip aaa send-id</b> command.	yes
Fax-Auth-Status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.	yes
Fax-Connect-Speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.	yes
Fax-Coverpage-Flag	Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.	yes
Fax-Dsn-Address	Indicates the address to which DSNs will be sent.	yes
Fax-Dsn-Flag	Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.	yes
Fax-Mdn-Address	Indicates the address to which MDNs will be sent.	yes
Fax-Mdn-Flag	Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.	yes

Attribute	Description	IOS XE 2.1
Fax-Modem-Time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.	yes
Fax-Msg-Id=	Indicates a unique fax message identification number assigned by Store and Forward Fax.	yes
Fax-Pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.	yes
Fax-Process-Abort- Flag	Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.	yes
Fax-Recipient-Count	Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.	yes
Gateway-Id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name	yes
mlp-links-max	Gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated.	yes
mlp-sess-id	Reports the identification number of the multilink bundle when the session closes. This attribute applies to sessions that are part of a multilink bundle. This attribute is sent in authentication-response packets.	yes

Attribute	Description	IOS XE 2.1
nas-rx-speed	Specifies the average number of bits per second over the course of the connection's lifetime. This attribute is sent in accounting-stop records.	yes
nas-tx-speed	Reports the transmit speed negotiated by the two modems.	yes
paks_in	The number of input packets transferred during this connection.	yes
paks_out	The number of output packets transferred during this connection.	yes
port	The port the user was logged in to.	yes
Port-Used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.	yes
pre-bytes-in	Records the number of input bytes before authentication. This attribute is sent in accounting-stop records.	yes
pre-bytes-out	Records the number of output bytes before authentication. This attribute is sent in accounting-stop records.	yes
pre-paks-in	Records the number of input packets before authentication. This attribute is sent in accounting-stop records.	yes
pre-paks-out	Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.	yes
pre-session-time	Specifies the length of time, in seconds, from when a call first connects to when it completes authentication.	yes
priv_level	The privilege level associated with the action.	yes

Attribute	Description	IOS XE 2.1
protocol	The protocol associated with the action.	yes
reason	Information included in the accounting packet that describes the event that caused a system change. Events described are system reload, system shutdown, or when accounting is reconfigured (turned on or off).	yes
service	The service the user used.	yes
start_time	The time the action started (in seconds since the epoch, 12:00 a.m. Jan 1 1970). The clock must be configured to receive this information.	yes
stop_time	The time the action stopped (in seconds since the epoch.) The clock must be configured to receive this information.	yes
task_id	Start and stop records for the same event must have matching (unique) task_id numbers.	yes
timezone	The time zone abbreviation for all timestamps included in this packet.	yes
xmit-rate	This AV pair has been renamed. See nas-tx-speed.	

The following table lists the cause codes and descriptions for the Disconnect Cause Extended (disc-cause-ext) attribute.

**Table 5**      **Disconnect Cause Extensions**

Cause Codes	Description	IOS XE 2.1
1000 - No Reason	No reason for the disconnect.	yes
1001 - No Disconnect	The event was not a disconnect.	yes
1002 - Unknown	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.	yes

Cause Codes	Description	IOS XE 2.1
1003 - Call Disconnect	The call has disconnected.	yes
1004 - CLID Auth Fail	Calling line ID (CLID) authentication has failed.	yes
1009 - No Modem Available	The modem is not available.	yes
1010 - No Carrier	The modem never detected data carrier detect (DCD). This code can appear if a disconnect occurs during the initial modem connection.	yes
1011 - Lost Carrier	The modem detected DCD but became inactive. This code can appear if a disconnect occurs during the initial modem connection.	yes
1012 - No Modem Results	The result codes could not be parsed. This code can appear if a disconnect occurs during the initial modem connection.	yes
1020 - TS User Exit	The user exited normally from the terminal server. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1021 - Idle Timeout	The user exited from the terminal server because the idle timer expired. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1022 - TS Exit Telnet	The user exited normally from a Telnet session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes

Cause Codes	Description	IOS XE 2.1
1023 - TS No IP Addr	The user could not switch to Serial Line Internet Protocol (SLIP) or PPP because the remote host had no IP address or because the dynamic pool could not assign one. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1024 - TS TCP Raw Exit	The user exited normally from a raw TCP session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1025 - TS Bad Password	The login process ended because the user failed to enter a correct password after three attempts. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1026 - TS No TCP Raw	The raw TCP option is not enabled. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1027 - TS CNTL-C	The login process ended because the user typed Ctrl-C. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1028 - TS Session End	The terminal server session has ended. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1029 - TS Close Vconn	The user closed the virtual connection. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1030 - TS End Vconn	The virtual connection has ended. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes

Cause Codes	Description	IOS XE 2.1
1031 - TS Rlogin Exit	The user exited normally from an Rlogin session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1032 - TS Rlogin Opt Invalid	The user selected an invalid Rlogin option. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1033 - TS Insuff Resources	The access server has insufficient resources for the terminal server session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	yes
1040 - PPP LCP Timeout	PPP link control protocol (LCP) negotiation timed out while waiting for a response from a peer. This code concerns PPP connections.	yes
1041 - PPP LCP Fail	There was a failure to converge on PPP LCP negotiations. This code concerns PPP connections.	yes
1042 - PPP Pap Fail	PPP Password Authentication Protocol (PAP) authentication failed. This code concerns PPP connections.	yes
1043 - PPP CHAP Fail	PPP Challenge Handshake Authentication Protocol (CHAP) authentication failed. This code concerns PPP connections.	yes
1044 - PPP Remote Fail	Authentication failed from the remote server. This code concerns PPP sessions.	yes
1045 - PPP Receive Term	The peer sent a PPP termination request. This code concerns PPP connections.	yes
PPP LCP Close (1046)	LCP got a close request from the upper layer while LCP was in an open state. This code concerns PPP connections.	yes



Cause Codes	Description	IOS XE 2.1
1047 - PPP No NCP	LCP closed because no NCPs were open. This code concerns PPP connections.	yes
1048 - PPP MP Error	LCP closed because it could not determine to which Multilink PPP bundle that it should add the user. This code concerns PPP connections.	yes
1049 - PPP Max Channels	LCP closed because the access server could not add any more channels to an MP session. This code concerns PPP connections.	yes
1050 - TS Tables Full	The raw TCP or Telnet internal session tables are full. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	yes
1051 - TS Resource Full	Internal resources are full. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	yes
1052 - TS Invalid IP Addr	The IP address for the Telnet host is invalid. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	yes
1053 - TS Bad Hostname	The access server could not resolve the host name. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	yes

Cause Codes	Description	IOS XE 2.1
1054 - TS Bad Port	The access server detected a bad or missing port number. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	yes
1060 - TCP Reset	The host reset the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1061 - TCP Connection Refused	The host refused the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1062 - TCP Timeout	The TCP connection timed out. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1063 - TCP Foreign Host Close	A foreign host closed the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1064 - TCP Net Unreachable	The TCP network was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1065 - TCP Host Unreachable	The TCP host was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1066 - TCP Net Admin Unreachable	The TCP network was administratively unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes

Cause Codes	Description	IOS XE 2.1
1067 - TCP Host Admin Unreachable	The TCP host was administratively unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1068 - TCP Port Unreachable	The TCP port was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	yes
1100 - Session Timeout	The session timed out because there was no activity on a PPP link. This code applies to all session types.	yes
1101 - Security Fail	The session failed for security reasons. This code applies to all session types.	yes
1102 - Callback	The session ended for callback. This code applies to all session types.	yes
1120 - Unsupported	One end refused the call because the protocol was disabled or unsupported. This code applies to all session types.	yes
1150 - Radius Disc	The RADIUS server requested the disconnect.	yes
1151 - Local Admin Disc	The local administrator has disconnected.	yes
1152 - SNMP Disc	Simple Network Management Protocol (SNMP) has disconnected.	yes
1160 - V110 Retries	The allowed retries for V110 synchronization have been exceeded.	yes
1170 - PPP Auth Timeout	Authentication timeout. This code applies to PPP sessions.	yes
1180 - Local Hangup	The call disconnected as the result of a local hangup.	yes

Cause Codes	Description	IOS XE 2.1
1185 - Remote Hangup	The call disconnected because the remote end hung up.	yes
1190 - T1 Quiesced	The call disconnected because the T1 line that carried it was quiesced.	yes
1195 - Call Duration	The call disconnected because the call duration exceeded the maximum amount of time allowed by the Max Call Mins or Max DS0 Mins parameter on the access server.	yes
1600 - VPDN User Disconnect	The user disconnected. This value applies to virtual private dial-up network (VPDN) sessions.	yes
1601 - VPDN Carrier Loss	Carrier loss has occurred. This code applies to VPDN sessions.	yes
1602 - VPDN No Resources	There are no resources. This code applies to VPDN sessions.	yes
1603 - VPDN Bad Control Packet	The control packet is invalid. This code applies to VPDN sessions.	yes
1604 - VPDN Admin Disconnect	The administrator disconnected. This code applies to VPDN sessions.	yes
1605 - VPDN Tunnel Down/ Setup Fail	The tunnel is down or the setup failed. This code applies to VPDN sessions.	yes
1606 - VPDN Local PPP Disconnect	There was a local PPP disconnect. This code applies to VPDN sessions.	yes
1607 - VPDN Softshut/Session Limit	New sessions cannot be established on the VPN tunnel. This code applies to VPDN sessions.	yes
1608 - VPDN Call Redirected	The call was redirected. This code applies to VPDN sessions.	yes
1801 - Q850 Unassigned Number	The number has not been assigned. This code applies to ISDN or modem calls that came in over ISDN.	no

Cause Codes	Description	IOS XE 2.1
1802 - Q850 No Route	The equipment that is sending this code has received a request to route the call through a particular transit network that it does not recognize. The equipment that is sending this code does not recognize the transit network because either the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment that is sending this code. This code applies to ISDN or modem calls that came in over ISDN.	no
1803 - Q850 No Route To Destination	The called party cannot be reached because the network through which the call has been routed does not serve the destination that is desired. This code applies to ISDN or modem calls that came in over ISDN.	no
1806 - Q850 Channel Unacceptable	The channel that has been most recently identified is not acceptable to the sending entity for use in this call. This code applies to ISDN or modem calls that came in over ISDN.	no
1816 - Q850 Normal Clearing	The call is being cleared because one of the users who is involved in the call has requested that the call be cleared. This code applies to ISDN or modem calls that came in over ISDN.	no
1817 - Q850 User Busy	The called party is unable to accept another call because the user-busy condition has been encountered. This code may be generated by the called user or by the network. In the case of the user, the user equipment is compatible with the call. This code applies to ISDN or modem calls that came in over ISDN.	no

Cause Codes	Description	IOS XE 2.1
1818 - Q850 No User Responding	Used when a called party does not respond to a call-establishment message with either an alerting or connect indication within the prescribed period of time that was allocated. This code applies to ISDN or modem calls that came in over ISDN.	no
1819 - Q850 No User Answer	The called party has been alerted but does not respond with a connect indication within a prescribed period of time. This code applies to ISDN or modem calls that came in over ISDN.	no
1821 - Q850 Call Rejected	The equipment that is sending this code does not wish to accept this call although it could have accepted the call because the equipment that is sending this code is neither busy nor incompatible. This code may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection. This code applies to ISDN or modem calls that came in over ISDN.	no
1822 - Q850 Number Changed	The number that is indicated for the called party is no longer assigned. The new called party number may optionally be included in the diagnostic field. This code applies to ISDN or modem calls that came in over ISDN.	no

Cause Codes	Description	IOS XE 2.1
1827 - Q850 Destination Out of Order	The destination that was indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term “not functioning correctly” indicates that a signaling message was unable to be delivered to the remote party. This code applies to ISDN or modem calls that came in over ISDN.	no
1828 - Q850 Invalid Number Format	The called party cannot be reached because the called party number is not in a valid format or is not complete. This code applies to ISDN or modem calls that came in over ISDN.	no
1829 - Q850 Facility Rejected	This code is returned when a supplementary service that was requested by the user cannot be provided by the network. This code applies to ISDN or modem calls that have come in over ISDN.	no
1830 - Q850 Responding to Status Enquiry	This code is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message. This code applies to ISDN or modem calls that came in over ISDN.	no
1831 - Q850 Unspecified Cause	No other code applies. This code applies to ISDN or modem calls that came in over ISDN.	no
1834 - Q850 No Circuit Available	No circuit or channel is available to handle the call. This code applies to ISDN or modem calls that came in over ISDN.	no

Cause Codes	Description	IOS XE 2.1
1838 - Q850 Network Out of Order	The network is not functioning correctly and the condition is likely to last a relatively long period of time. This code applies to ISDN or modem calls that came in over ISDN.	no
1841 - Q850 Temporary Failure	The network is not functioning correctly and the condition is not likely to last a long period of time. This code applies to ISDN or modem calls that came in over ISDN.	no
1842 - Q850 Network Congestion	The network is congested. This code applies to ISDN or modem calls that came in over ISDN.	no
1843 - Q850 Access Info Discarded	This code indicates that the network could not deliver access information to the remote user as requested. This code applies to ISDN or modem calls that came in over ISDN.	no
1844 - Q850 Requested Channel Not Available	This code is returned when the circuit or channel that is indicated by the requesting entity cannot be provided by the other side of the interface. This code applies to ISDN or modem calls that came in over ISDN.	no
1845 - Q850 Call Pre-empted	The call was preempted. This code applies to ISDN or modem calls that came in over ISDN.	no
1847 - Q850 Resource Unavailable	This code is used to report a resource-unavailable event only when no other code in the resource-unavailable class applies. This code applies to ISDN or modem calls that came in over ISDN.	no
1850 - Q850 Facility Not Subscribed	Not a subscribed facility. This code applies to ISDN or modem calls that came in over ISDN.	no



Cause Codes	Description	IOS XE 2.1
1852 - Q850 Outgoing Call Barred	Although the calling party is a member of the closed user group for the outgoing closed user group call, outgoing calls are not allowed for this member. This code applies to ISDN or modem calls that came in over ISDN.	no
Q850 Incoming Call Barred (1854)	Although the called party is a member of the closed user group for the incoming closed user group call, incoming calls are not allowed to this member. This code applies to ISDN or modem calls that have come in over ISDN.	no
1858 - Q850 Bearer Capability Not Available	The user has requested a bearer capability that is implemented by the equipment that generated this code but that is not available at this time. This code applies to ISDN or modem calls that have come in over ISDN.	no
1863 - Q850 Service Not Available	The code is used to report a service- or option-not-available event only when no other code in the service- or option-not-available class applies. This code applies to ISDN or modem calls that have come in over ISDN.	no
1865 - Q850 Bearer Capability Not Implemented	The equipment that is sending this code does not support the bearer capability that was requested. This code applies to ISDN or modem calls that have come in over ISDN.	no
1866 - Q850 Channel Not Implemented	The equipment that is sending this code does not support the channel type that was requested. This code applies to ISDN or modem calls that have come in over ISDN.	no

Cause Codes	Description	IOS XE 2.1
1869 - Q850 Facility Not Implemented	The supplementary service requested by the user cannot be provided by the network. This code applies to ISDN or modem calls that have come in over ISDN.	no
1881 - Q850 Invalid Call Reference	The equipment that is sending this code has received a message having a call reference that is not currently in use on the user-network interface. This code applies to ISDN or modem calls that have come in over ISDN.	no
1882 - Q850 Channel Does Not Exist	The channel most recently identified is not acceptable to the sending entity for use in this call. This code applies to ISDN or modem calls that have come in over ISDN. This code applies to ISDN or modem calls that have come in over ISDN.	no
1888 - Q850 Incompatible Destination	The equipment that is sending this code has received a request to establish a call that has low-layer compatibility or other compatibility attributes that cannot be accommodated. This code applies to ISDN or modem calls that have come in over ISDN.	no
1896 - Q850 Mandatory Info Element Is Missing	The equipment that is sending this code has received a message that is missing an information element that must be present in the message before that message can be processed. This code applies to ISDN or modem calls that have come in over ISDN.	no

Cause Codes	Description	IOS XE 2.1
1897 - Q850 Non Existent Message Type	The equipment that is sending this code has received a message with a message type that it does not recognize either because this is a message that is not defined or that is defined but not implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.	no
1898 - Q850 Invalid Message	This code is used to report an invalid message when no other code in the invalid message class applies. This code applies to ISDN or modem calls that have come in over ISDN.	no
1899 - Q850 Bad Info Element	The information element not recognized. This code applies to ISDN or modem calls that have come in over ISDN.	no
1900 - Q850 Invalid Element Contents	The equipment that is sending this code has received an information element that it has implemented; however, one or more fields in the information element are coded in such a way that has not been implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.	no
1901 - Q850 Wrong Message for State	The message that was received is incompatible with the call state. This code applies to ISDN or modem calls that have come in over ISDN.	no
1902 - Q850 Recovery on Timer Expiration	A procedure has been initiated by the expiration of a timer in association with error-handling procedures. This code applies to ISDN or modem calls that have come in over ISDN.	no

Cause Codes	Description	IOS XE 2.1
1903 - Q850 Info Element Error	The equipment that is sending this code has received a message that includes information elements or parameters that are not recognized because the information element identifiers or parameter names are not defined or are defined but not implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.	no
1911 - Q850 Protocol Error	This code is used to report a protocol error event only when no other code in the protocol error class applies. This code applies to ISDN or modem calls that have come in over ISDN.	no
1927 - Q850 Unspecified Internetworking Event	There has been an error when interworking with a network that does not provide codes for actions that it takes. This code applies to ISDN or modem calls that have come in over ISDN.	no

For more information about configuring TACACS+ accounting, see the Configuring TACACS+ feature module.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.