



Configuring TACACS+

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

- [Finding Feature Information, on page 1](#)
- [Prerequisites for TACACS+, on page 1](#)
- [Restrictions for TACACS+, on page 2](#)
- [Information About TACACS+, on page 3](#)
- [How to Configure TACACS+, on page 27](#)
- [Configuration Examples for TACACS+, on page 37](#)
- [Additional References for TACACS+, on page 41](#)
- [Feature Information for TACACS+, on page 41](#)

Finding Feature Information

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <https://cfng.cisco.com/>. An account on Cisco.com is not required.

Prerequisites for TACACS+

The following are the prerequisites for set up and configuration of switch access with TACACS+ (must be performed in the order presented):

1. Configure the switches with the TACACS+ server addresses.
2. Set an authentication key.
3. Configure the key from Step 2 on the TACACS+ servers.
4. Enable authentication, authorization, and accounting (AAA).

5. Create a login authentication method list.
6. Apply the list to the terminal lines.
7. Create an authorization and accounting method list.

The following are the prerequisites for controlling switch access with TACACS+:

- You must have access to a configured TACACS+ server to configure TACACS+ features on your switch. Also, you must have access to TACACS+ services maintained in a database on a TACACS+ daemon typically running on a LINUX or Windows workstation.
- We recommend a redundant connection between a switch stack and the TACACS+ server. This is to help ensure that the TACACS+ server remains accessible in case one of the connected stack members is removed from the switch stack.
- You need a system running the TACACS+ daemon software to use TACACS+ on your switch.
- To use TACACS+, it must be enabled.
- Authorization must be enabled on the switch to be used.
- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- To use any of the AAA commands listed in this section or elsewhere, you must first enable AAA with the **aaa new-model** command.
- At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting.
- The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all ports except those that have a named method list explicitly defined. A defined method list overrides the default method list.
- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Restrictions for TACACS+

TACACS+ can be enabled only through AAA commands.

Information About TACACS+

TACACS+ and Switch Access

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



Note Beginning with Cisco IOS Release 15.2(7)E3, the legacy command **tacacs-server** is deprecated. Use the **tacacs server** command if the software running on your device is Cisco IOS Release 15.2(7)E3 or later releases.

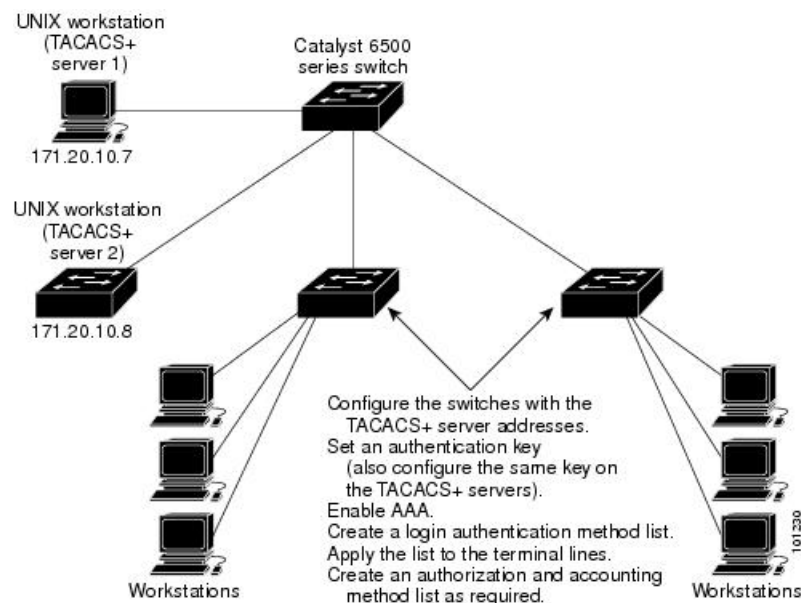
TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch.

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 method for managing multiple network access points from a single management service. Your switch can be a network access server along with other Cisco routers and access servers.

Figure 1: Typical TACACS+ Network Configuration



TACACS+, administered through the AAA security services, can provide these services:

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

The authentication facility can conduct a dialog with the user (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send 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 can 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 switch and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the switch and the TACACS+ daemon are encrypted.

TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a switch using TACACS+, this process occurs:

1. When the connection is established, the switch contacts the TACACS+ daemon to obtain a username prompt to show to the user. The user enters a username, and the switch then contacts the TACACS+ daemon to obtain a password prompt. The switch displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

TACACS+ allows a dialog between the daemon and the user until the daemon receives enough information to authenticate the user. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.

2. The switch eventually receives one of these responses from the TACACS+ daemon:
 - **ACCEPT**—The user is authenticated and service can begin. If the switch is configured to require authorization, authorization begins at this time.
 - **REJECT**—The user is not authenticated. The user can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
 - **ERROR**—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the switch. If an ERROR response is received, the switch typically tries to use an alternative method for authenticating the user.
 - **CONTINUE**—The user is prompted for additional authentication information.

After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. 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 contains data in the form of attributes that direct the EXEC or NETWORK session for that user and the services that the user can access:
 - Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
 - Connection parameters, including the host or client IP address, access list, and user timeouts

Method List

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

If a method list is configured under VTY lines, the corresponding method list must be added to AAA. The following example shows how to configure a method list under a VTY line:

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

The following example shows how to configure a method list in AAA:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```

If no method list is configured under VTY lines, the default method list must be added to AAA. The following example shows a VTY configuration without a method list:

```
Device# configure terminal
Device(config)# line vty 0 4
```

The following example shows how to configure the default method list:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+
```

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.

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 1: Supported TACACS+ Authentication and Authorization AV Pairs

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
acl=x	ASCII number representing a connection access list. Used only when service=shell.	yes	yes	yes	yes	yes	yes	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	yes	yes	yes	yes	yes	yes
addr-pool=x	Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip. Note that addr-pool 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 ip-local pool command to declare local pools. For example: 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 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.	yes	yes	yes	yes	yes	yes	yes
autocmd=x	Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet example.com). Used only with service=shell.	yes	yes	yes	yes	yes	yes	yes
callback- dialstring	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.	no	yes	yes	yes	yes	yes	yes
callback-line	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.	no	yes	yes	yes	yes	yes	yes
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.	no	yes	yes	yes	yes	yes	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. Note This TACACS+ AV pair cannot be used with RADIUS attribute 26.	yes	yes	yes	yes	yes	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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. Note This TACACS+ AV pair cannot be used with RADIUS attribute 26.	yes	yes	yes	yes	yes	yes	yes
data-service	Used with the service=outbound and protocol=ip.	no	no	no	no	no	yes	yes
dial-number	Defines the number to dial. Used with the service=outbound and protocol=ip.	no	no	no	no	no	yes	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.	no	no	no	yes	yes	yes	yes
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.	no	no	no	no	no	yes	yes
gw-password	Specifies the password for the home gateway during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes	yes	yes
idletime=x	Sets a value, in minutes, after which an idle session is terminated. A value of zero indicates no timeout.	no	yes	yes	yes	yes	yes	yes
inacl#<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.	no	no	no	yes	yes	yes	yes
inacl=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	yes	yes	yes	yes	yes	yes
interface-config#<n>	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. Note This attribute replaces the "interface-config=" attribute.	no	no	no	yes	yes	yes	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.	no	no	yes	yes	yes	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
l2tp-busy-disconnect	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.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
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.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
l2tp-hidden-avp	When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
l2tp-tunnel- authen	If this attribute is set, it performs L2TP tunnel authentication. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-tunnel-password	Shared secret used for L2TP tunnel authentication and AVP hiding. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
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.	no	no	no	no	no	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
link-compression=	Defines whether to turn on or turn off “stac” compression over a PPP link. Used with service=ppp. Link compression is defined as a numeric value as follows: <ul style="list-style-type: none"> • 0: None • 1: Stac • 2: Stac-Draft-9 • 3: MS-Stac 	no	no	no	yes	yes	yes	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.	no	no	no	yes	yes	yes	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.	no	no	no	no	no	yes	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.	no	no	no	yes	yes	yes	yes
min-links	Sets the minimum number of links for MLP. Used with service=ppp and protocol=multilink, protocol=vpdn.	no	no	no	no	no	yes	yes
nas-password	Specifies the password for the network access server during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes	yes	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.	no	yes	yes	yes	yes	yes	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	yes	yes	yes	yes	yes	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	yes	yes	yes	yes	yes	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	yes	yes	yes	yes	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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.	no	no	no	yes	yes	yes	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 (PPP/IP only)	yes	yes	yes	yes	yes	yes
pool-def#<n>	Defines IP address pools on the network access server. Used with service=ppp and protocol=ip.	no	no	no	yes	yes	yes	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.	no	no	yes	yes	yes	yes	yes
port-type	Indicates the type of physical port the network access server is using to authenticate the user. Physical ports are indicated by a numeric value as follows: <ul style="list-style-type: none"> • 0: Asynchronous • 1: Synchronous • 2: ISDN-Synchronous • 3: ISDN-Asynchronous (V.120) • 4: ISDN- Asynchronous (V.110) • 5: Virtual Used with service=any and protocol=aaa.	no	no	no	no	no	yes	yes
ppp-vj-slot-compression	Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.	no	no	no	yes	yes	yes	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	yes	yes	yes	yes	yes	yes
protocol=x	A protocol that is a subset of a service. An example would be any PPP NCP. Currently known values are lcp , ip , ipx , atalk , vines , lat , xremote , tn3270 , telnet , rlogin , pad , vpdn , osicp , deccp , ccp , cdp , bridging , xns , nbf , bap , multilink , and unknown .	yes	yes	yes	yes	yes	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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.	no	no	no	no	no	yes	yes
route	Specifies a route to be applied to an interface. Used with service=slip, service=ppp, and protocol=ip. During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows: route="dst_address mask [gateway]" 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 ip route configuration command on a network access server. If <i>gateway</i> is omitted, the peer's address is the gateway. The route is expunged when the connection terminates.	no	yes	yes	yes	yes	yes	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.	no	no	no	yes	yes	yes	yes
routing=x	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).	yes	yes	yes	yes	yes	yes	yes
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.	no	no	no	yes	yes	yes	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.	no	no	no	yes	yes	yes	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.	no	no	no	yes	yes	yes	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.	no	no	no	yes	yes	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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.	no	no	no	yes	yes	yes	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.	no	no	no	no	no	yes	yes
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.	no	no	no	no	no	yes	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 slip , ppp , arap , shell , tty-daemon , connection , and system . This attribute must always be included.	yes	yes	yes	yes	yes	yes	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 vpdn outgoing global configuration command.	no	no	yes	yes	yes	yes	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 ip mobile secure host <addr> 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.	no	no	no	no	no	yes	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	yes	yes	yes	yes	yes	yes
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 vpdn outgoing command. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes	yes	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.	no	no	no	yes	yes	yes	yes
zonelist=x	A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5).	yes	yes	yes	yes	yes	yes	yes

See Configuring TACACS+ module for the documents used to configure TACACS+, and TACACS+ authentication and authorization.

TACACS Accounting AV Pairs

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

Table 2: Supported TACACS+ Accounting AV Pairs

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
Abort-Cause	If the fax session is terminated, indicates the system component that signaled the termination. Examples of system components that could trigger a termination are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.	no	no	no	no	no	yes	yes
bytes_in	The number of input bytes transferred during this connection.	yes	yes	yes	yes	yes	yes	yes
bytes_out	The number of output bytes transferred during this connection.	yes	yes	yes	yes	yes	yes	yes
Call-Type	Describes the type of fax activity: fax receive or fax send.	no	no	no	no	no	yes	yes
cmd	The command the user executed.	yes	yes	yes	yes	yes	yes	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.	no	no	no	yes	yes	yes	yes
disc-cause-ext	Extends the disc-cause attribute to support vendor-specific reasons why a connection was taken off-line.	no	no	no	yes	yes	yes	yes
elapsed_time	The elapsed time in seconds for the action. Useful when the device does not keep real time.	yes	yes	yes	yes	yes	yes	yes
Email-Server-Address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
event	Information included in the accounting packet that describes a state change in the router. Events described are accounting starting and accounting stopping.	yes	yes	yes	yes	yes	yes	yes
Fax-Account-Id-Origin	Indicates the account ID origin as defined by system administrator for the mmoip aaa receive-id or the mmoip aaa send-id command.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
Fax-Dsn-Address	Indicates the address to which DSNs will be sent.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
Fax-Mdn-Address	Indicates the address to which MDNs will be sent.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
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.	no	no	no	no	no	yes	yes
Fax-Msg-Id=	Indicates a unique fax message identification number assigned by Store and Forward Fax.	no	no	no	no	no	yes	yes
Fax-Pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.	no	no	no	no	no	yes	yes
Fax-Process-Abort-Flag	Indicates that the fax session was terminated or successful. True means that the session was terminated; false means that the session was successful.	no	no	no	no	no	yes	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.	no	no	no	no	no	yes	yes
Gateway-Id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name	no	no	no	no	no	yes	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.	no	no	no	yes	yes	yes	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.	no	no	no	yes	yes	yes	yes
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.	no	no	no	yes	yes	yes	yes
nas-tx-speed	Reports the transmit speed negotiated by the two modems.	no	no	no	yes	yes	yes	yes
paks_in	The number of input packets transferred during this connection.	yes	yes	yes	yes	yes	yes	yes

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
paks_out	The number of output packets transferred during this connection.	yes	yes	yes	yes	yes	yes	yes
port	The port the user was logged in to.	yes	yes	yes	yes	yes	yes	yes
Port-Used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.	no	no	no	no	no	yes	yes
pre-bytes-in	Records the number of input bytes before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
pre-bytes-out	Records the number of output bytes before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
pre-paks-in	Records the number of input packets before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
pre-paks-out	Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
pre-session-time	Specifies the length of time, in seconds, from when a call first connects to when it completes authentication.	no	no	no	yes	yes	yes	yes
priv_level	The privilege level associated with the action.	yes	yes	yes	yes	yes	yes	yes
protocol	The protocol associated with the action.	yes	yes	yes	yes	yes	yes	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	yes	yes	yes	yes	yes	yes
service	The service the user used.	yes	yes	yes	yes	yes	yes	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	yes	yes	yes	yes	yes	yes
stop_time	The time the action stopped (in seconds since the epoch.) The clock must be configured to receive this information.	yes	yes	yes	yes	yes	yes	yes
task_id	Start and stop records for the same event must have matching (unique) task_id numbers.	yes	yes	yes	yes	yes	yes	yes
timezone	The time zone abbreviation for all timestamps included in this packet.	yes	yes	yes	yes	yes	yes	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 3: Disconnect Cause Extensions

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1000 - No Reason	No reason for the disconnect.	no	no	no	no	yes	yes	yes	yes
1001 - No Disconnect	The event was not a disconnect.	no	no	no	no	yes	yes	yes	yes
1002 - Unknown	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.	no	no	no	no	yes	yes	yes	yes
1003 - Call Disconnect	The call has disconnected.	no	no	no	no	yes	yes	yes	yes
1004 - CLID Auth Fail	Calling line ID (CLID) authentication has failed.	no	no	no	no	yes	yes	yes	yes
1009 - No Modem Available	The modem is not available.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
1011 - Lost Carrier	The modem detected DCD but became inactive. This code can appear if a disconnect occurs during the initial modem connection.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
1041 - PPP LCP Fail	There was a failure to converge on PPP LCP negotiations. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1042 - PPP Pap Fail	PPP Password Authentication Protocol (PAP) authentication failed. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1043 - PPP CHAP Fail	PPP Challenge Handshake Authentication Protocol (CHAP) authentication failed. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1044 - PPP Remote Fail	Authentication failed from the remote server. This code concerns PPP sessions.	no	no	no	no	yes	yes	yes	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1045 - PPP Receive Term	The peer sent a PPP termination request. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
1047 - PPP No NCP	LCP closed because no NCPs were open. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1062 - TCP Timeout	The TCP connection timed out. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
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.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
1100 - Session Timeout	The session timed out because there was no activity on a PPP link. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1101 - Security Fail	The session failed for security reasons. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1102 - Callback	The session ended for callback. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1120 - Unsupported	One end refused the call because the protocol was disabled or unsupported. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1150 - Radius Disc	The RADIUS server requested the disconnect.	no	no	no	no	yes	yes	yes	yes
1151 - Local Admin Disc	The local administrator has disconnected.	no	no	no	no	yes	yes	yes	yes
1152 - SNMP Disc	Simple Network Management Protocol (SNMP) has disconnected.	no	no	no	no	yes	yes	yes	yes
1160 - V110 Retries	The allowed retries for V110 synchronization have been exceeded.	no	no	no	no	yes	yes	yes	yes
1170 - PPP Auth Timeout	Authentication timeout. This code applies to PPP sessions.	no	no	no	no	yes	yes	yes	yes
1180 - Local Hangup	The call disconnected as the result of a local hangup.	no	no	no	no	yes	yes	yes	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1185 - Remote Hangup	The call disconnected because the remote end hung up.	no	no	no	no	yes	yes	yes	yes
1190 - T1 Quiesced	The call disconnected because the T1 line that carried it was quiesced.	no	no	no	no	yes	yes	yes	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.	no	no	no	no	yes	yes	yes	yes
1600 - VPDN User Disconnect	The user disconnected. This value applies to virtual private dial-up network (VPDN) sessions.	no	no	no	no	no	no	yes	yes
1601 - VPDN Carrier Loss	Carrier loss has occurred. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1602 - VPDN No Resources	There are no resources. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1603 - VPDN Bad Control Packet	The control packet is invalid. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1604 - VPDN Admin Disconnect	The administrator disconnected. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1605 - VPDN Tunnel Down/Setup Fail	The tunnel is down or the setup failed. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1606 - VPDN Local PPP Disconnect	There was a local PPP disconnect. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1607 - VPDN Softshut/Session Limit	New sessions cannot be established on the VPN tunnel. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1608 - VPDN Call Redirected	The call was redirected. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
1831 - Q850 Unspecified Cause	No other code applies. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
1842 - Q850 Network Congestion	The network is congested. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
1845 - Q850 Call Pre-empted	The call was preempted. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
1850 - Q850 Facility Not Subscribed	Not a subscribed facility. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes
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	no	no	no	no	no	no	yes

Configuring AAA Server Group Selection Based on DNIS

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

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

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

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

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

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

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

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



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

To configure the device 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:

Procedure

	Command or Action	Purpose
Step 1	Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	Device (config)# aaa dnis map enable	Enables DNIS mapping.
Step 4	Router(config)# aaa dnis map dnis-number authentication ppp group server-group-name	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
Step 5	Router(config)# aaa dnis map dnis-number accounting network [none start-stop stop-only] group server-group-name	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting.

TACACS+ Configuration Options

You can configure the switch to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

TACACS+ Login Authentication

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

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.

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.

TACACS+ Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.



Note Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

Per VRF for TACACS Servers

The Per VRF for TACACS+ Servers feature allows per virtual routing and forwarding (VRF) AAA to be configured on TACACS+ servers. TACACS+ server access is required to configure this feature.

How to Configure TACACS+

Identifying the TACACS+ Server Host and Setting the Authentication Key

Follow these steps to identify the TACACS+ server host and set the authentication key:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
Step 3	<p>tacacs server <i>servername</i></p> <p>Example:</p> <pre>Device(config)# tacacs server yourserver</pre>	Identifies the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them.
Step 4	<p>aaa new-model</p> <p>Example:</p> <pre>Device(config)# aaa new-model</pre>	Enables AAA.
Step 5	<p>aaa group server tacacs+ <i>group-name</i></p> <p>Example:</p> <pre>Device(config)# aaa group server tacacs+ your_server_group</pre>	<p>(Optional) Defines the AAA server-group with a group name.</p> <p>This command puts the Device in a server group subconfiguration mode.</p>
Step 6	<p>server <i>ip-address</i></p> <p>Example:</p> <pre>Device(config)# server 10.1.2.3</pre>	<p>(Optional) Associates a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group.</p> <p>Each server in the group must be previously defined in Step 3.</p>
Step 7	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 8	<p>show running-config</p> <p>Example:</p> <pre>Device# show running-config</pre>	Verifies your entries.
Step 9	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring TACACS+ Login Authentication

Follow these steps to configure TACACS+ login authentication:

Before you begin

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports.



Note To secure the for HTTP access by using AAA methods, you must configure the with the **ip http authentication aaa** global configuration command. Configuring AAA authentication does not secure the for HTTP access by using AAA methods.

For more information about the **ip http authentication** command, see the *Cisco IOS Security Command Reference, Release 12.4*.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables AAA.
Step 4	aaa authentication login {default list-name} method1 [method2...] Example: Device(config)# aaa authentication login default tacacs+ local	Creates a login authentication method list. <ul style="list-style-type: none"> • To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. • For <i>list-name</i>, specify a character string to name the list you are creating.

	Command or Action	Purpose
		<ul style="list-style-type: none"> For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. <p>Select one of these methods:</p> <ul style="list-style-type: none"> <i>enable</i>—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the enable password global configuration command. <i>group tacacs+</i>—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. <i>line</i> —Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the password password line configuration command. <i>local</i>—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command. <i>local-case</i>—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the username name password global configuration command. <i>none</i>—Do not use any authentication for login.
Step 5	line [console tty vty] <i>line-number</i> <i>[ending-line-number]</i> Example: <pre>Device(config)# line 2 4</pre>	Enters line configuration mode, and configures the lines to which you want to apply the authentication list.
Step 6	login authentication { default <i>list-name</i> } Example:	Applies the authentication list to a line or set of lines.

	Command or Action	Purpose
	Device(config-line)# login authentication default	<ul style="list-style-type: none"> • If you specify default, use the default list created with the aaa authentication login command. • For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 7	end Example: Device(config-line)# end	Returns to privileged EXEC mode.
Step 8	show running-config Example: Device# show running-config	Verifies your entries.
Step 9	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to privileged EXEC mode.



Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	aaa authorization network tacacs+ Example: Device (config)# <code>aaa authorization network tacacs+</code>	Configures the switch for user TACACS+ authorization for all network-related service requests.
Step 4	aaa authorization exec tacacs+ Example: Device (config)# <code>aaa authorization exec tacacs+</code>	Configures the switch for user TACACS+ authorization if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 5	end Example: Device (config)# <code>end</code>	Returns to privileged EXEC mode.
Step 6	show running-config Example: Device# <code>show running-config</code>	Verifies your entries.
Step 7	copy running-config startup-config Example: Device# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Starting TACACS+ Accounting

Follow these steps to start TACACS+ Accounting:

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa accounting network start-stop tacacs+ Example: Device(config)# aaa accounting network start-stop tacacs+	Enables TACACS+ accounting for all network-related service requests.
Step 4	aaa accounting exec start-stop tacacs+ Example: Device(config)# aaa accounting exec start-stop tacacs+	Enables TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 5	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 6	show running-config Example: Device# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to do next

To establish a session with a router if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Establishing a Session with a Router if the AAA Server is Unreachable

To establishing a session with a router if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Establishing a Session with a Router if the AAA Server is Unreachable

The **aaa accounting system guarantee-first** command guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

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:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip vrf vrf-name Example: Device(config)# ip vrf cisco	Configures a VRF table and enters VRF configuration mode.
Step 4	rd route-distinguisher Example:	Creates routing and forwarding tables for a VRF instance.

	Command or Action	Purpose
	Device(config-vrf)# rd 100:1	
Step 5	exit Example: Device(config-vrf)# exit	Exits VRF configuration mode.
Step 6	interface <i>interface-name</i> Example: Device(config)# interface Loopback0	Configures an interface and enters interface configuration mode.
Step 7	ip vrf forwarding <i>vrf-name</i> Example: Device(config-if)# ip vrf forwarding cisco	Configures a VRF for the interface.
Step 8	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.2 255.0.0.0	Sets a primary or secondary IP address for an interface.
Step 9	exit Example: Device(config-if)# exit	Exits interface configuration mode.
Step 10	aaa group server tacacs+ <i>group-name</i> Example: Device(config)# aaa group server tacacs+ tacacs1	Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 11	server-private <i>{ip-address name} [nat]</i> [single-connection] [port port-number] [timeout seconds] [key [0 7] string] Example: Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco	Configures the IP address of the private TACACS+ server for the group server.
Step 12	ip vrf forwarding <i>vrf-name</i> Example:	Configures the VRF reference of a AAA TACACS+ server group.

	Command or Action	Purpose
	Device(config-sg-tacacs)# ip vrf forwarding cisco	
Step 13	ip tacacs source-interface <i>subinterface-name</i> Example: Device(config-sg-tacacs)# ip tacacs source-interface Loopback0	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
Step 14	exit Example: Device(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.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug tacacs authentication Example: Device# debug tacacs authentication	Displays information about AAA/TACACS+ authentication.
Step 3	debug tacacs authorization Example: Device# debug tacacs authorization	Displays information about AAA/TACACS+ authorization.
Step 4	debug tacacs accounting Example: Device# debug tacacs accounting	Displays information about accountable events as they occur.

	Command or Action	Purpose
Step 5	debug tacacs packets Example: Device# debug tacacs packets	Displays information about TACACS+ packets.

Monitoring TACACS+

Table 4: Commands for Displaying TACACS+ Information

Command	Purpose
show tacacs	Displays TACACS+ server statistics.

Configuration Examples for TACACS+

Example: TACACS Authorization

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 secserver
  address ipv4 10.1.2.3
  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** command identifies the TACACS+ daemon 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.

Example: TACACS Accounting

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 secserver
  address ipv4 10.1.2.3
  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** command identifies the TACACS+ daemon 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.

Example: TACACS Authentication

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 secserver
  address ipv4 10.1.2.3
  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** 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 secserver
  address ipv4 10.1.2.3
  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** 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 secserver
  address ipv4 10.1.2.3
  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** 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 secserver
  address ipv4 10.2.3.4
  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** 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.”

Example: Configuring Per VRF for TACACS Servers

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 for TACACS+

Related Documents

Related Topic	Document Title
Cisco security commands	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
IPv6 commands	Cisco IOS IPv6 Command Reference

MIBs

MB	MIBs Link
	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for TACACS+

Release	Feature Information
Cisco IOS Release 15.0(2)EX	This feature was introduced.

Release	Feature Information
Cisco IOS 12.2(54)SG Cisco IOS 15.2(1)E	The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers. The following commands were introduced or modified: ip tacacs source-interface , ip vrf forwarding (server-group) , server-private (TACACS+) .
Cisco IOS 15.2(7)E3	The legacy command tacacs-server is deprecated. Use the new tacacs server command.