



Configuring Accounting

The AAA accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) 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, and auditing.

- [Prerequisites for Configuring Accounting, on page 1](#)
- [Restrictions for Configuring Accounting, on page 1](#)
- [Information About Configuring Accounting, on page 2](#)
- [How to Configure AAA Accounting, on page 10](#)
- [Configuration Examples for AAA Accounting, on page 17](#)

Prerequisites for Configuring Accounting

The following tasks must be performed before configuring accounting using named method lists:

- Enable AAA on the network access server by using the **aaa new-model** command in global configuration mode.
- Define the characteristics of the RADIUS or TACACS+ security server if RADIUS or TACACS+ authorization is issued. For more information about configuring the Cisco network access server to communicate with the RADIUS security server, see the Configuring RADIUS module. For more information about configuring the Cisco network access server to communicate with the TACACS+ security server, see the Configuring TACACS+ module.

Restrictions for Configuring Accounting

- Accounting information can be sent simultaneously to a maximum of only four AAA servers.

Information About Configuring Accounting

Named Method Lists for Accounting

Similar to authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed.

Named accounting method lists allow particular security protocol to be designated and used on specific lines or interfaces for accounting services. The only exception is the default method list (which is named default). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is simply a named list describing the accounting methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists allow one or more security protocols to be designated and used for accounting, thus ensuring a backup system for accounting in case the initial method fails. Cisco IOS software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS software selects the next accounting method listed in the method list. This process continues until there is successful communication with a listed accounting method, or all methods defined are exhausted.



Note The Cisco IOS software attempts accounting with the next listed accounting method only when there is no response from the previous method. If accounting fails at any point in this cycle--meaning that the security server responds by denying the user access--the accounting process stops and no other accounting methods are attempted.

Accounting method lists are specific to the type of accounting being requested. AAA supports seven different types of accounting:

- **EXEC:** Provides information about user EXEC terminal sessions of the network access server.
- **Commands:** Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Connection:** Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
- **System:** Provides information about system-level events.
- **Resource:** Provides “start” and “stop” records for calls that have passed user authentication, and provides “stop” records for calls that fail to authenticate.
- **VRRS:** Provides information about Virtual Router Redundancy Service (VRRS).



Note System accounting does not use named accounting lists; only the default list for system accounting can be defined.

When a named method list is created, a particular list of accounting methods for the indicated accounting type are defined.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named “default”). If the **aaa accounting** command for a particular accounting type is issued without specifying a named method list, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined (A defined method list overrides the default method list). If no default method list is defined, then no accounting takes place.

This section includes the following subsections:

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 comprise the group of RADIUS servers. T1 and T2 comprise the group of TACACS+ servers.

In Cisco IOS software, RADIUS and TACACS+ server configurations are global. A subset of the configured server hosts can be specified using server groups. These server groups can be used for a particular service. For example, server groups allow R1 and R2 to be defined as separate server groups (SG1 and SG2), and T1 and T2 as separate server groups (SG3 and SG4). This means either R1 and T1 (SG1 and SG3) or R2 and T2 (SG2 and SG4) can be specified in the method list, which provides more flexibility in the way that RADIUS and TACACS+ resources are assigned.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server from the same IP address. If two different host entries on the same RADIUS server are configured for the same service: for example, accounting; the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services (The RADIUS host entries are tried in the order in which they are configured).

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, see the “Configuring RADIUS” or “Configuring TACACS+” modules.

AAA Accounting Methods

The following two methods of accounting are supported:

- **TACACS+:** The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.
- **RADIUS:** The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.



Note Passwords and accounting logs are masked before being sent to the TACACS+ or RADIUS security servers. Use the **aaa accounting commands visible-keys** command to send unmasked information to the TACACS+ or RADIUS security servers.

Accounting Record Types

For minimal accounting, use the **stop-only** keyword, which instructs the specified method (**RADIUS** or **TACACS+**) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the **start-stop** keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the **none** keyword.

Accounting Methods

The table below lists the supported accounting methods.

Table 1: AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for accounting.
group tacacs+	Uses the list of all TACACS+ servers for accounting.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> .

The method argument refers to the actual method the authentication algorithm tries. Additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all other methods return an error, specify additional methods in the command. For example, to create a method list named `acct_tac1` that specifies RADIUS as the backup method of authentication in the event that TACACS+ authentication returns an error, enter the following command:

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

To create a default list that is used when a named list is not specified in the **aaa accounting** command, use the **default** keyword followed by the methods that are wanted to be used in default situations. The default method list is automatically applied to all interfaces.

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa accounting network default stop-only group radius
```

AAA Accounting supports the following methods:

- **group tacacs** : To have the network access server send accounting information to a TACACS+ security server, use the **group tacacs+ method** keyword.
- **group radius** : To have the network access server send accounting information to a RADIUS security server, use the **group radius method** keyword.
- **group** *group-name* : To specify a subset of RADIUS or TACACS+ servers to use as the accounting method, use the **aaa accounting** command with the **group group-name** method. To specify and define

the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group loginrad**:

```
aaa group server radius loginrad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the **group loginrad**.

To specify **group loginrad** as the method of network accounting when no other method list has been defined, enter the following command:

```
aaa accounting network default start-stop group loginrad
```

Before a group name can be used as the accounting method, communication with the RADIUS or TACACS+ security server must be enabled.

AAA Accounting Types

EXEC Accounting

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.

The following example shows the information contained in a RADIUS EXEC accounting record for a dial-in user:

```
Wed Jun 27 04:26:23 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000006"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:27:25 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000006"
Acct-Session-Time = 62
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

```

Wed Jun 27 03:46:21 2001      172.16.25.15      username1      tty3      5622329430/4327528
start
  task_id=2      service=shell
Wed Jun 27 04:08:55 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop
  task_id=2      service=shell      elapsed_time=1354

```

The following example shows the information contained in a RADIUS EXEC accounting record for a Telnet user:

```

Wed Jun 27 04:48:32 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 26
  User-Name = "username1"
  Caller-ID = "10.68.202.158"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000010"
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 26
  User-Name = "username1"
  Caller-ID = "10.68.202.158"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000010"
  Acct-Session-Time = 14
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"

```

The following example shows the information contained in a TACACS+ EXEC accounting record for a Telnet user:

```

Wed Jun 27 04:06:53 2001      172.16.25.15      username1      tty26      10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001      172.16.25.15      username1      tty26      10.68.202.158
stoptask_id=41      service=shell      elapsed_time=9

```

Command Accounting

Command accounting provides information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the user who executed it.

The following example shows the information contained in a TACACS+ command accounting record for privilege level 1:

```

Wed Jun 27 03:46:47 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=3      service=shell      priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=4      service=shell      priv-lvl=1      cmd=show interfaces Ethernet 0
<cr>
Wed Jun 27 03:47:03 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=5      service=shell      priv-lvl=1      cmd=show ip route <cr>

```

The following example shows the information contained in a TACACS+ command accounting record for privilege level 15:

```
Wed Jun 27 03:47:17 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=6      service=shell      priv-lvl=15      cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=7      service=shell      priv-lvl=15      cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=8      service=shell      priv-lvl=15      cmd=ip address 10.1.1.1 255.255.255.0
<cr>
```



Note The Cisco implementation of RADIUS does not support command accounting.

Connection Accounting

Connection accounting provides information about all outbound connections made from the network access server such as Telnet, LAT, TN3270, PAD, and rlogin.

The following example shows the information contained in a RADIUS connection accounting record for an outbound Telnet connection:

```
Wed Jun 27 04:28:00 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "00000008"
Login-Service = Telnet
Login-IP-Host = "10.68.202.158"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:28:39 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "00000008"
Login-Service = Telnet
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 10774
Acct-Output-Octets = 112
Acct-Input-Packets = 91
Acct-Output-Packets = 99
Acct-Session-Time = 39
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound Telnet connection:

```
Wed Jun 27 03:47:43 2001      172.16.25.15      username1  tty3      5622329430/4327528
start   task_id=10      service=connection      protocol=telnet addr=10.68.202.158 cmd=telnet
        username1-sun
Wed Jun 27 03:48:38 2001      172.16.25.15      username1  tty3      5622329430/4327528
stop    task_id=10      service=connection      protocol=telnet addr=10.68.202.158 cmd=telnet
        username1-sun      bytes_in=4467 bytes_out=96      paks_in=61      paks_out=72 elapsed_time=55
```

The following example shows the information contained in a RADIUS connection accounting record for an outbound rlogin connection:

```
Wed Jun 27 04:29:48 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Input-Octets = 18686
        Acct-Output-Octets = 86
        Acct-Input-Packets = 90
        Acct-Output-Packets = 68
        Acct-Session-Time = 22
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound rlogin connection:

```
Wed Jun 27 03:48:46 2001      172.16.25.15      username1  tty3      5622329430/4327528
start   task_id=12      service=connection      protocol=rlogin addr=10.68.202.158 cmd=rlogin
        username1-sun /user username1
Wed Jun 27 03:51:37 2001      172.16.25.15      username1  tty3      5622329430/4327528
stop    task_id=12      service=connection      protocol=rlogin addr=10.68.202.158 cmd=rlogin
        username1-sun /user username1 bytes_in=659926 bytes_out=138      paks_in=2378      paks_
out=1251      elapsed_time=171
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound LAT connection:

```

Wed Jun 27 03:53:06 2001      172.16.25.15  username1  tty3  5622329430/4327528
start task_id=18 service=connection protocol=lat addr=VAX cmd=lat
VAX
Wed Jun 27 03:54:15 2001      172.16.25.15  username1  tty3  5622329430/4327528
stop task_id=18 service=connection protocol=lat addr=VAX cmd=lat
VAX bytes_in=0 bytes_out=0 paks_in=0 paks_out=0 elapsed_time=6

```

System Accounting

System accounting provides information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

The following accounting record shows a typical TACACS+ system accounting record server indicating that AAA Accounting has been turned off:

```

Wed Jun 27 03:55:32 2001      172.16.25.15  unknown unknown unknown start task_id=25
service=system
event=sys_acct reason=reconfigure

```



Note The precise format of accounting packets records may vary depending on the TACACS+ daemon.

The following accounting record shows a TACACS+ system accounting record indicating that AAA Accounting has been turned on:

```

Wed Jun 27 03:55:22 2001      172.16.25.15  unknown unknown unknown stop task_id=23
service=system
event=sys_acct reason=reconfigure

```

AAA Accounting Enhancements

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:

- Statistics for each AAA function (when used in conjunction with the **show radius statistics** command)

- Status of servers providing AAA functions
- Identities of external AAA servers
- Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call

The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

Table 2: SNMP End-User Data Objects

SessionId	The session identification used by the AAA Accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).
UserId	The user login ID or zero-length string if a login is unavailable.
IpAddr	The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.
IdleTime	The elapsed time in seconds that the session has been idle.
Disconnect	The session termination object used to disconnect the given client.
CallId	The entry index corresponding to this accounting session that the Call Tracker record stored.

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

Table 3: SNMP AAA Session Summary

ActiveTableEntries	Number of sessions currently active.
ActiveTableHighWaterMark	Maximum number of sessions present at once since last system reinstallation.
TotalSessions	Total number of sessions since last system reinstallation.
DisconnectedSessions	Total number of sessions that have been disconnected using since last system reinstallation.

Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ AV pairs or RADIUS attributes, depending on which security method is implemented.

How to Configure AAA Accounting

Configuring AAA Accounting Using Named Method Lists

To configure AAA Accounting using named method lists, perform the following steps:



Note System accounting does not use named method lists. For system accounting, define only the default method list.

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	aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [method1 [method2...]] Example: Device(config)# aaa accounting system default start-stop	Creates an accounting method list and enables accounting. The argument <i>list-name</i> is a character string used to name the created list.
Step 4	Do one of the following: • line [aux console tty vty] line-number [ending-line-number] • interface interface-type interface-number Example: Device(config)# line aux line1	Enters the line configuration mode for the lines to which the accounting method list is applied. or Enters the interface configuration mode for the interfaces to which the accounting method list is applied.
Step 5	accounting {arap commands level connection exec} {default list-name} Example: Device(config-line)# accounting arap default	Applies the accounting method list to a line or set of lines.
Step 6	end Example: Device(config-line)# end	(Optional) Exits line configuration mode and returns to privileged EXEC mode.

Suppressing Generation of Accounting Records for Null Username Sessions

When AAA Accounting is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this

is users who come in on lines where the **aaa authentication login method-list none** command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command in global configuration mode:

Command	Purpose
Device(config)# aaa accounting suppress null-username	Prevents accounting records from being generated for users whose username string is NULL.

Generating Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, use the following command in global configuration mode:

Command	Purpose
Device(config)# aaa accounting update [newinfo] [periodic] <i>number</i>	Enables periodic interim accounting records to be sent to the accounting server.

When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records are sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the *number* argument. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.



Caution

Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network.

Configuring an Alternate Method to Enable Periodic Accounting Records

You can use the following alternative method to enable periodic interim accounting records to be sent to the accounting server.

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	aaa accounting network default Example: Device(config)# aaa accounting network default	Configures the default accounting for all network-related service requests and enters accounting method list configuration mode.
Step 4	action-type {none start-stop [periodic {disable interval minutes}] stop-only} Example: Device(cfg-acct-mlist)# action-type start-stop periodic interval 5	Specifies the type of action to be performed on accounting records. • (Optional) The periodic keyword specifies periodic accounting action. • The interval keyword specifies the periodic accounting interval. • The <i>value</i> argument specifies the intervals for accounting update records (in minutes). • The disable keyword disables periodic accounting.
Step 5	end Example: Device(cfg-acct-mlist)# end	Exits accounting method list configuration mode and returns to privileged EXEC mode.

Generating Interim Service Accounting Records

Perform this task to enable the generation of interim service accounting records at periodic intervals for subscribers.

Before you begin

RADIUS Attribute 85 in the user service profile always takes precedence over the configured interim-interval value. RADIUS Attribute 85 must be in the user service profile. See the RADIUS Attributes Overview and RADIUS IETF Attributes feature document for more information.



Note If RADIUS Attribute 85 is not in the user service profile, then the interim-interval value configured in Generating Interim Accounting Records is used for service interim accounting records.

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	subscriber service accounting interim-interval <i>minutes</i> Example: Device(config)# subscriber service accounting interim-interval 10	Enables the generation of interim service accounting records at periodic intervals for subscribers. The <i>minutes</i> argument indicates the number of periodic intervals to send accounting update records from 1 to 71582 minutes.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Generating Accounting Records for a Failed Login or Session

When AAA accounting is activated, the Cisco IOS XE software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication.

To specify that accounting stop records be generated for users who fail to authenticate at login or during session negotiation, use the following command in global configuration mode:

Command or Action	Purpose
aaa accounting send stop-record authentication failure	Generates “stop” records for users who fail to authenticate at login or during session negotiation.

Suppressing System Accounting Records over Switchover

To suppress the system accounting-on and accounting-off messages during switchover, use the following command in global configuration mode:

Command or Action	Purpose
aaa accounting redundancy suppress system-records	Suppresses the system accounting messages during switchover.

Configuring AAA Resource Failure Stop Accounting

To enable resource failure stop accounting, use the following command in global configuration mode:

Command	Purpose
<pre>Device(config)# aaa accounting resource method-list stop-failure group server-group</pre>	Generates a “stop” record for any calls that do not reach user authentication. Note Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 1 section must be performed, and SNMP must be enabled on the network access server.

Configuring AAA Resource Accounting for Start-Stop Records

To enable full resource accounting for start-stop records, use the following command in global configuration mode:

Command	Purpose
<pre>Device(config)# aaa accounting resource method-list start-stop group server-group</pre>	Supports the ability to send a “start” record at each call setup, followed with a corresponding “stop” record at the call disconnect. Note Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 1 section must be performed, and SNMP must be enabled on the network access server.

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

Configuring Per-DNIS AAA Broadcast Accounting

To configure AAA broadcast accounting per DNIS, use the **aaa dnis map accounting network** command in global configuration mode:

Command	Purpose
Device(config)# aaa dnis map <i>dnis-number</i> accounting network [start-stop stop-only none] [broadcast] <i>method1</i> [<i>method2...</i>]	Allows per-DNIS accounting configuration. This command has precedence over the global aaa accounting command. Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Establishing a Session with a Device if the AAA Server Is Unreachable

To establish a console session with a device if the AAA server is unreachable, use the following command in global configuration mode:

Command or Action	Purpose
no aaa accounting system guarantee-first	The aaa accounting system guarantee-first command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes. To resolve this problem, use the no aaa accounting system guarantee-first command.

Monitoring Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users logged in, use the following command in privileged EXEC mode:

Command or Action	Purpose
show accounting	Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.

Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

Command or Action	Purpose
debug aaa accounting	Displays information on accountable events as they occur.

Configuration Examples for AAA Accounting

Example: Configuring a Named Method List

The following example shows how to configure a Cisco device (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login admins local
Device(config)# aaa authorization network network1 group radius local
Device(config)# aaa accounting network network2 start-stop group radius group tacacs+
Device(config)# username root password ALongPassword
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.31.255.0
Device(config-server-tacacs)# key goaway
Device(config-server-tacacs)# exit
Device(config)# radius server isp
Device(config-sg-radius)# key myRaDiUSpassWoRd
Device(config-sg-radius)# exit
Device(config)# line 1 16
Device(config-line)# autoselect during-login
Device(config-line)# login authentication admins
Device(config-line)# modem dialin
Device(config-line)# end
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines a method list, “admins”, for login authentication.
- The **tacacs server** command defines the name of the TACACS+ server host.
- The **key** command defines the shared secret text string between the network access server and the TACACS+ server host.
- The **radius server** command defines the name of the RADIUS server host.
- The **key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **login authentication admins** command applies the admins method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to accept only incoming calls.

The table below describes the fields contained in the preceding output.

Table 4: show accounting Field Descriptions

Field	Description
Active Accounted actions on	Terminal line or interface name user with which the user logged in.
User	User's ID.
Priv	User's privilege level.
Task ID	Unique identifier for each accounting session.
Accounting Record	Type of accounting session.
Elapsed	Length of time (hh:mm:ss) for this session type.
attribute=value	AV pairs associated with this accounting session.

Example: Configuring AAA Broadcast Accounting

The following example shows how to turn on broadcast accounting using the global **aaa accounting** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa group server radius isp
Device(config-sg-radius)# server 10.0.0.1
Device(config-sg-radius)# server 10.0.0.2
Device(config-sg-radius)# exit
Device(config)# aaa group server tacacs+ isp_customer
Device config-sg-tacacs+)# server 172.0.0.1
Device config-sg-tacacs+)# exit
Device(config)# aaa accounting network default start-stop broadcast group isp group
isp_customer
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.0.0.1
Device(config-server-tacacs)# key key2
Device(config-server-tacacs)# end
```

The **broadcast** keyword causes “start” and “stop” accounting records for network connections to be sent simultaneously to server 10.0.0.1 in the group **isp** and to server 172.0.0.1 in the group **isp_customer**. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group **isp_customer**.

Example: Configuring per-DNIS AAA Broadcast Accounting

The following example shows how to turn on per-DNIS broadcast accounting using the global **aaa dnis map accounting network** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa group server radius isp
Device(config-sg-radius)# server 10.0.0.1
Device(config-sg-radius)# server 10.0.0.2
Device(config-sg-radius)# exit
Device(config)# aaa group server tacacs+ isp_customer
```

```
Device config-sg-tacacs+)# server 172.0.0.1
Device config-sg-tacacs+)# exit
Device(config)# aaa dnis map enable
Device(config)# aaa dnis map 7777 accounting network start-stop broadcast group isp group
isp_customer
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.0.0.1
Device(config-server-tacacs)# key key_2
Device(config-server-tacacs)# end
```

The **broadcast** keyword causes “start” and “stop” accounting records for network connection calls having DNIS number 7777 to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

