



Configuring Accounting

First Published: October 26, 1998

Last Updated: November 24, 2010

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Configuring Accounting”](#) section on page 35.

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

Contents

- [Prerequisites for Configuring Accounting, page 2](#)
- [Restrictions for Configuring Accounting, page 2](#)
- [Information About Configuring Accounting, page 2](#)
- [How to Configure AAA Accounting, page 18](#)
- [Configuration Examples for AAA Accounting, page 28](#)
- [Additional References, page 33](#)
- [Feature Information for Configuring Accounting, page 35](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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.
- For Service Selection Gateway (SSG) systems, the **aaa accounting network broadcast** command broadcasts only **start-stop** accounting records. If interim accounting records are configured using the **ssg accounting interval** command, the interim accounting records are sent only to the configured default RADIUS server.

Information About Configuring Accounting

- [Named Method Lists for Accounting, page 2](#)
- [AAA Accounting Types, page 6](#)
- [AAA Accounting Enhancements, page 16](#)
- [Accounting Attribute-Value Pairs, page 18](#)

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:

- **Network**—Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.
- **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.

Once again, 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.

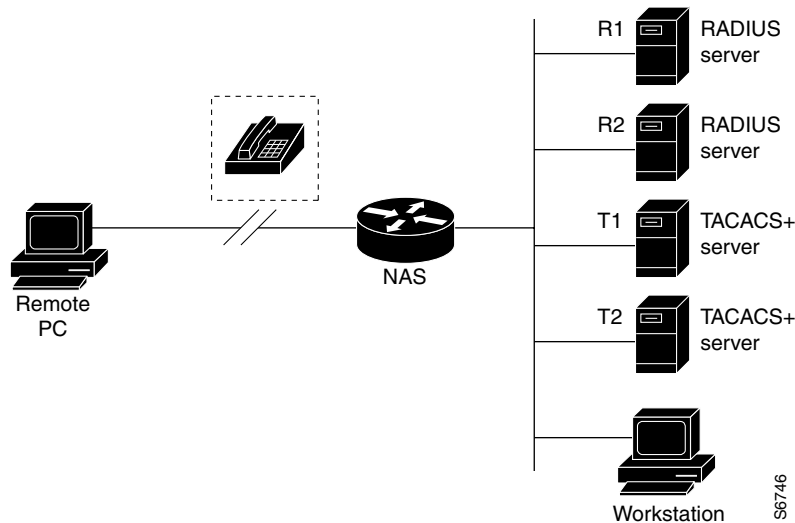
This section includes the following subsections:

- [Method Lists and Server Groups, page 4](#)
- [AAA Accounting Methods, page 5](#)
- [Accounting Record Types, page 5](#)
- [Accounting Methods, page 5](#)

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. [Figure 1](#) 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.

Figure 1 Typical AAA Network Configuration



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+” module in the *Cisco IOS Security Configuration Guide: Securing User Services*.

AAA Accounting Methods

The Cisco IOS software supports the following two methods for accounting:

- **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.

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

Table 11 lists the supported accounting methods.

Table 11 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.

**Note**

Accounting method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for accounting applies.

- **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

AAA supports the following seven different accounting types:

- [Network Accounting, page 6](#)
- [System Accounting, page 12](#)
- [Resource Accounting, page 13](#)
- [Connection Accounting, page 11](#)
- [System Accounting, page 12](#)
- [Resource Accounting, page 13](#)
- [VRRS Accounting, page 15](#)

Network Accounting

Network accounting provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through an EXEC session:

```
Wed Jun 27 04:44:45 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 5
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
```

```
Caller-ID = "562"  
Acct-Status-Type = Start  
Acct-Authentic = RADIUS  
Service-Type = Exec-User  
Acct-Session-Id = "0000000D"  
Acct-Delay-Time = 0  
User-Id = "username1"  
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:45:00 2001  
NAS-IP-Address = "172.16.25.15"  
NAS-Port = 5  
User-Name = "username1"  
Client-Port-DNIS = "4327528"  
Caller-ID = "562"  
Acct-Status-Type = Start  
Acct-Authentic = RADIUS  
Service-Type = Framed  
Acct-Session-Id = "0000000E"  
Framed-IP-Address = "10.1.1.2"  
Framed-Protocol = PPP  
Acct-Delay-Time = 0  
User-Id = "username1"  
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:47:46 2001  
NAS-IP-Address = "172.16.25.15"  
NAS-Port = 5  
User-Name = "username1"  
Client-Port-DNIS = "4327528"  
Caller-ID = "562"  
Acct-Status-Type = Stop  
Acct-Authentic = RADIUS  
Service-Type = Framed  
Acct-Session-Id = "0000000E"  
Framed-IP-Address = "10.1.1.2"  
Framed-Protocol = PPP  
Acct-Input-Octets = 3075  
Acct-Output-Octets = 167  
Acct-Input-Packets = 39  
Acct-Output-Packets = 9  
Acct-Session-Time = 171  
Acct-Delay-Time = 0  
User-Id = "username1"  
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:48:45 2001  
NAS-IP-Address = "172.16.25.15"  
NAS-Port = 5  
User-Name = "username1"  
Client-Port-DNIS = "4327528"  
Caller-ID = "408"  
Acct-Status-Type = Stop  
Acct-Authentic = RADIUS  
Service-Type = Exec-User  
Acct-Session-Id = "0000000D"  
Acct-Delay-Time = 0  
User-Id = "username1"  
NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who first started an EXEC session:

```
Wed Jun 27 04:00:35 2001 172.16.25.15  username1  tty4  562/4327528
starttask_id=28      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15  username1  tty4  562/4327528  starttask_id=30
addr=10.1.1.1  service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15  username1  tty4  408/4327528  update
task_id=30      addr=10.1.1.1  service=ppp  protocol=ip  addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15  username1  tty4  562/4327528
stoptask_id=30      addr=10.1.1.1  service=ppp  protocol=ip  addr=10.1.1.1
bytes_in=2844      bytes_out=1682  paks_in=36  paks_out=24  elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15  username1  tty4  562/4327528
stoptask_id=28      service=shell  elapsed_time=57
```

**Note**

The precise format of accounting packets records may vary depending on the security server daemon.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:30:52 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 3
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "562"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Framed
  Acct-Session-Id = "0000000B"
  Framed-Protocol = PPP
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:36:49 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 3
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "562"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Framed
  Acct-Session-Id = "0000000B"
  Framed-Protocol = PPP
  Framed-IP-Address = "10.1.1.1"
  Acct-Input-Octets = 8630
  Acct-Output-Octets = 5722
  Acct-Input-Packets = 94
  Acct-Output-Packets = 64
  Acct-Session-Time = 357
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:02:19 2001 172.16.25.15  username1  Async5  562/4327528
starttask_id=35      service=ppp
```



```

Wed Jun 27 04:02:25 2001 172.16.25.15  username1  Async5  562/4327528  update
task_id=35      service=ppp      protocol=ip      addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15  username1  Async5  562/4327528
stoptask_id=35      service=ppp      protocol=ip      addr=10.1.1.2  bytes_in=3366
bytes_out=2149      paks_in=42      paks_out=28      elapsed_time=164

```

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
```

Additional tasks for measuring system resources are covered in the Cisco IOS software configuration guides. For example, IP accounting tasks are described in the “[Configuring IP Services](#)” chapter in the *Cisco IOS Application Services Configuration Guide*.

Resource Accounting

The Cisco implementation of AAA accounting provides “start” and “stop” record support for calls that have passed user authentication. The additional feature of generating “stop” records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

This section includes the following subsections:

- [AAA Resource Failure Stop Accounting, page 13](#)
- [AAA Resource Accounting for Start-Stop Records, page 15](#)

AAA Resource Failure Stop Accounting

Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.

This functionality generates a “stop” accounting record for any calls that do not reach user authentication; “stop” records are generated from the moment of call setup. All calls that pass user authentication behave as they did before; that is, no additional accounting records are seen.

[Figure 2](#) illustrates a call setup sequence with normal call flow (no disconnect) and without AAA resource failure stop accounting enabled.

Figure 2 Modem Dial-In Call Setup Sequence With Normal Flow and Without Resource Failure Stop Accounting Enabled

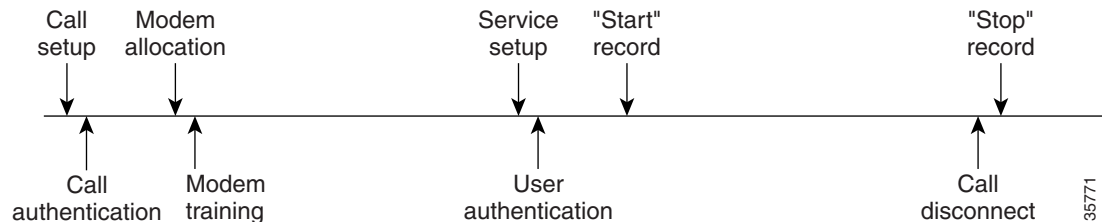


Figure 3 illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

Figure 3 *Modem Dial-In Call Setup Sequence With Normal Flow and With Resource Failure Stop Accounting Enabled*

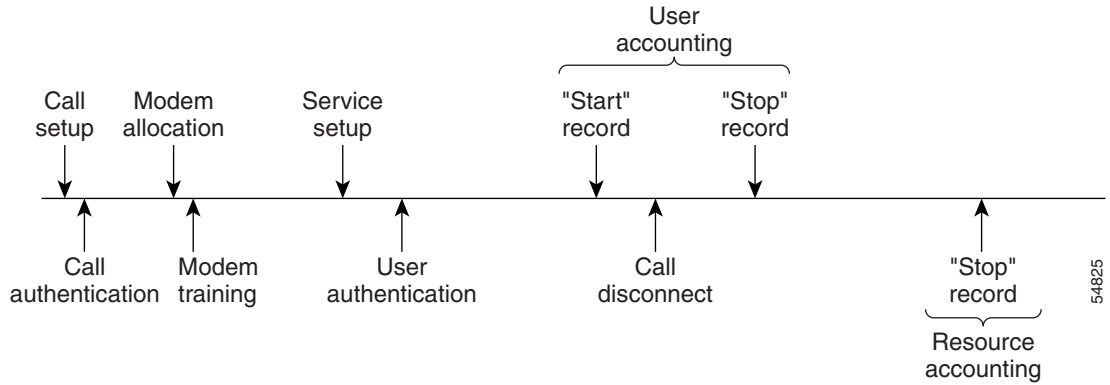


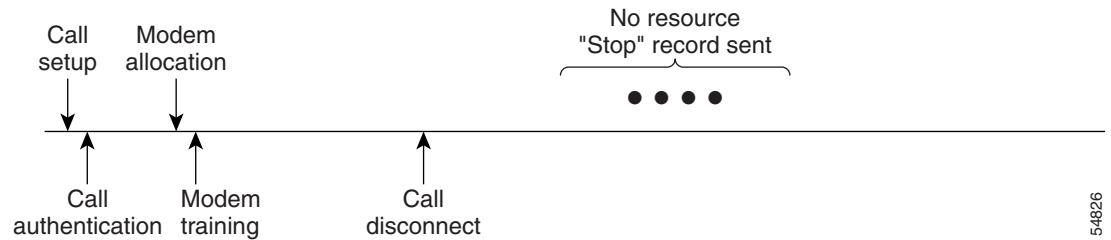
Figure 4 illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

Figure 4 *Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and With Resource Failure Stop Accounting Enabled*



Figure 5 illustrates a call setup sequence with call disconnect occurring before user authentication and without AAA resource failure stop accounting enabled.

Figure 5 *Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and Without Resource Failure Stop Accounting Enabled*



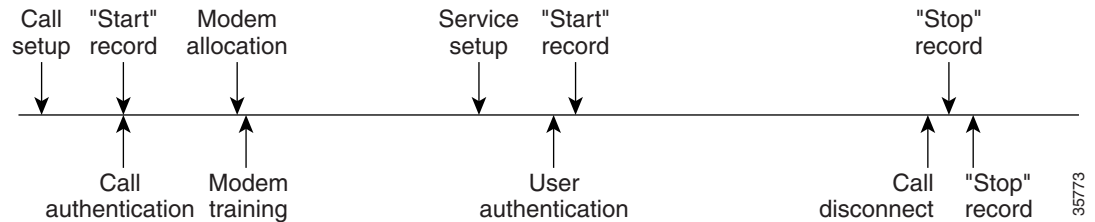
AAA Resource Accounting for Start-Stop Records

AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

With this feature, a call setup and call disconnect “start-stop” accounting record tracks the progress of the resource connection to the device. A separate user authentication “start-stop” accounting record tracks the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

Figure 6 illustrates a call setup sequence with AAA resource start-stop accounting enabled.

Figure 6 *Modem Dial-In Call Setup Sequence With Resource Start-Stop Accounting Enabled*



VRRS Accounting

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client. The VRRS multiclient service provides a consistent interface with FHRP protocols by abstracting over several FHRPs and providing an idealized view of their state. VRRS manages data updates, allowing interested clients to register in one place and receive updates for named FHRP groups or all registered FHRP groups.

Virtual Router Redundancy Protocol (VRRP) is an FHRP that acts as a server that pushes FHRP status information out to all registered VRRS clients. Clients obtain status on essential information provided by the FHRP, including current and previous redundancy states, active and inactive L3 and L2 addresses, and, in some cases, information about other redundant gateways in the network. Clients can use this information to provide stateless and stateful redundancy information to clients and protocols.

VRRS Accounting Plug-in

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state. The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode.

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state.

The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode. The VRRS Accounting plug-in sends an accounting-on message to RADIUS when a VRRS group transitions to the master state, and it sends an accounting-off message when a VRRS group transitions from the master state.

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, VRRS Name
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Time
- Attribute 44, Acct-Session-Id

Accounting messages for a VRRS transitioning out of master state are sent after all PPPoE accounting stop messages for sessions that are part of that VRRS.

AAA Accounting Enhancements

- [AAA Broadcast Accounting, page 16](#)
- [AAA Session MIB, page 17](#)

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



Note

This command is supported only on Cisco AS5300 and Cisco AS5800 universal access server platforms.

Table 12 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 12 *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.

Table 13 describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

Table 13 *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, page 19](#)
- [Suppressing Generation of Accounting Records for Null Username Sessions, page 21](#)
- [Generating Interim Accounting Records, page 22](#)
- [Generating Accounting Records for Failed Login or Session, page 22](#)
- [Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records, page 23](#)
- [Configuring AAA Resource Failure Stop Accounting, page 23](#)
- [Configuring AAA Resource Accounting for Start-Stop Records, page 23](#)
- [Configuring AAA Broadcast Accounting, page 24](#)
- [Configuring Per-DNIS AAA Broadcast Accounting, page 24](#)
- [Configuring AAA Session MIB, page 24](#)
- [Configuring VRRS Accounting, page 26](#)
- [Establishing a Session with a Router if the AAA Server is Unreachable, page 27](#)
- [Monitoring Accounting, page 28](#)
- [Troubleshooting Accounting, page 28](#)

Configuring AAA Accounting Using Named Method Lists

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting** {system | network | exec | connection | commands *level*} {default | *list-name*} {start-stop | stop-only | none} [*method1* [*method2*...]]
4. **line** [aux | console | tty | vty] *line-number* [*ending-line-number*]
5. **accounting** {arap | commands *level* | connection | exec} {default | *list-name*}
6. **end**



Note

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

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# aaa accounting {system network exec connection commands <i>level</i> } {default <i>list-name</i> } {start-stop stop-only none} [<i>method1</i> [<i>method2</i> ...]] Example: Router(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	Router(config)# line [aux console tty vty] <i>line-number</i> [<i>ending-line-number</i>] or Router(config)# interface <i>interface-type</i> <i>interface-number</i> Example: Router(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.

	Command	Purpose
Step 5	<pre>Router(config-line)# accounting {arap commands level connection exec} {default <i>list-name</i>}</pre> <p>or</p> <pre>Router(config-if)# ppp accounting {default <i>list-name</i>}</pre> <p>Example: Router(config-line)# <code>accounting arap default</code></p>	<p>Applies the accounting method list to a line or set of lines.</p> <p>or</p> <p>Applies the accounting method list to an interface or set of interfaces.</p>
Step 6	<pre>Router(config-line)# end</pre> <p>Example: Router(config-line)# <code>end</code></p>	<p>(Optional) Exits line configuration mode and returns to global configuration mode.</p>

This section includes the following subsection:

- [Configuring RADIUS System Accounting, page 20](#)

Configuring RADIUS System Accounting

Perform this task to configure RADIUS system accounting on the global RADIUS server:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `radius-server accounting system host-config`
5. `aaa group server radius server-name`
6. `server-private {host-name | ip-address} key {[0 server-key | 7 server-key] server-key}`
7. `accounting system host-config`
8. `end`

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables AAA network security services.
Step 4	radius-server accounting system host-config Example: Router(config)# radius-server accounting system host-config	Enables the router to send a system accounting record for the addition and deletion of a RADIUS server.
Step 5	aaa group server radius server-name Example: Router(config)# aaa group server radius radgroup1	Adds the RADIUS server and enters server-group configuration mode. <ul style="list-style-type: none"> The <i>server-name</i> argument specifies the RADIUS server group name.
Step 6	server-private { <i>host-name</i> <i>ip-address</i> } key {[0 <i>server-key</i> 7 <i>server-key</i>] <i>server-key</i> Example: Router(config-sg-radius)# server-private 172.16.1.11 key cisco	Enters the hostname or IP address of the RADIUS server and hidden server key. <ul style="list-style-type: none"> (Optional) 0 with the <i>server-key</i> argument specifies that an unencrypted (cleartext) hidden server key follows. (Optional) 7 with the <i>server-key</i> argument specifies that an encrypted hidden server key follows. The <i>server-key</i> argument specifies the hidden server key. If the <i>server-key</i> argument is configured without the 0 or 7 preceding it, it is unencrypted. <p>Note Once the server-private command is configured, RADIUS system accounting is enabled.</p>
Step 7	accounting system host-config Example: Router(config-sg-radius)# accounting system host-config	Enables the generation of system accounting records for private server hosts when they are added or deleted.
Step 8	end Example: Router(config-sg-radius)# end	Exits server-group (config-sg-radius) configuration mode and returns to global configuration 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
Router(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
Router(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.

Generating Accounting Records for Failed Login or Session

When AAA Accounting is activated, the Cisco IOS software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication but fail PPP negotiation for some reason.

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	Purpose
Router(config)# aaa accounting send stop-record authentication failure	Generates “stop” records for users who fail to authenticate at login or during session negotiation using PPP.
Router(config)# aaa accounting send stop-record always	Sends authentication, authorization, and accounting (AAA) stop records regardless of whether a start record was sent earlier.

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, you can specify the NETWORK records to be generated before EXEC-stop records. In cases such as billing customers for specific services, it can be desirable to keep network start and stop records together, essentially “nesting” them within the framework of the EXEC start and stop messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

To nest accounting records for user sessions, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa accounting nested	Nests network accounting records.

Configuring AAA Resource Failure Stop Accounting

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

Command	Purpose
Router(config)# aaa accounting resource <i>method-list stop-failure group server-group</i>	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” section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see the “Configuring SNMP Support” chapter in the <i>Cisco IOS Network Management Configuration Guide</i> .

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
Router(config)# aaa accounting resource method-list start-stop group server-group	<p>Supports the ability to send a “start” record at each call setup, followed with a corresponding “stop” record at the call disconnect.</p> <p>Note Before configuring this feature, the tasks described in the “Prerequisites for Configuring Accounting” section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see the “Configuring SNMP Support” chapter in the <i>Cisco IOS Network Management Configuration Guide</i>.</p> <p>Note</p>

Configuring AAA Broadcast Accounting

To configure AAA broadcast accounting, use the `aaa accounting` command in global configuration mode:

Command	Purpose
Router(config)# aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [broadcast] method1 [method2...]	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.

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
Router(config)# aaa dnis map dnis-number accounting network [start-stop stop-only none] [broadcast] method1 [method2...]	<p>Allows per-DNIS accounting configuration. This command has precedence over the global <code>aaa accounting</code> command.</p> <p>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.</p>

Configuring AAA Session MIB

The following tasks must be performed before configuring the AAA session MIB feature:

- Configure SNMP. For information on SNMP, see the chapter “[Configuring SNMP Support](#)” in the *Cisco IOS Network Management Configuration Guide*.
- Configure AAA.
- Define the RADIUS or TACACS+ server characteristics.

**Note**

Overusing SNMP can affect the overall system performance; therefore, normal network management performance must be considered when this feature is used.

To configure AAA session MIB, use the following command in global configuration mode

	Command	Purpose
Step 1	Router(config)# aaa session-mib disconnect	Monitors and terminates authenticated client connections using SNMP. To terminate the call, the disconnect keyword must be used.

Configuring VRRS Accounting

Perform the following task to configure Virtual Router Redundancy Service (VRRS) to send AAA Accounting messages to the AAA server:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting vrrs {default | list-name} start-stop method1 [method2...]**
4. **aaa attribute list list-name**
5. **attribute type name value [service service] [protocol protocol] [mandatory] [tag tag-value]**
6. **exit**
7. **vrrs vrrs-group-name**
8. **accounting delay seconds**
9. **accounting method {default | accounting-method-list}**
10. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa accounting vrrs {default list-name} start-stop method1 [method2...] Example: Router(config)# aaa accounting vrrs default start-stop	Enables AAA accounting for VRRS.

	Command	Purpose
Step 4	aaa attribute list <i>list-name</i> Example: Router(config)# aaa attribute list list1	Defines a AAA attribute list locally on a router, and enters attribute list configuration mode.
Step 5	attribute type <i>name value</i> [service <i>service</i>] [protocol <i>protocol</i>][mandatory][tag <i>tag-value</i>] Example: Router(config-attr-list)# attribute type example 1	Defines an attribute type that is to be added to an attribute list locally on a router.
Step 6	exit Example: Router(config-attr-list)# exit	Exits attribute list configuration mode and returns to global configuration mode.
Step 7	vrrs <i>vrrs-group-name</i> Example: Router(config)# vrrs vrrs1	(Optional) Defines a VRRP group and configures parameters for the VRRS group, and enters VRRS configuration mode.
Step 8	accounting delay <i>seconds</i> Example: Router(config-vrrs)# accounting delay 10	(Optional) Specifies the delay time for sending accounting-off messages to the VRRS.
Step 9	accounting method { default <i>accounting-method-list</i> } Example: Router(config-vrrs)# accounting method default	(Optional) Enables VRRS accounting for a VRRP group.
Step 10	exit Example: Router(config-vrrs)# exit	Exits VRRS configuration mode.

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

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

Command	Purpose
Router(config)# no aaa accounting system guarantee-first	<p>The aaa accounting system guarantee-first command guarantees system accounting as the first record, which is the default condition.</p> <p>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, the no aaa accounting system guarantee-first command can be used.</p>



Note Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Monitoring Accounting

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

Command	Purpose
Router# 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	Purpose
Router# debug aaa accounting	Displays information on accountable events as they occur.

Configuration Examples for AAA Accounting

- [Example: Configuring Named Method List, page 29](#)
- [Example: Configuring AAA Resource Accounting, page 31](#)
- [Example: Configuring AAA Broadcast Accounting, page 31](#)
- [Example: Configuring Per-DNIS AAA Broadcast Accounting, page 31](#)

- [Example: AAA Session MIB, page 32](#)
- [Example: Configuring VRRS Accounting, page 32](#)

Example: Configuring Named Method List

The following example shows how to configure a Cisco AS5200 (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.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network blue1 group radius local
aaa accounting network red1 start-stop group radius group tacacs+

username root password ALongPassword

tacacs-server host 172.31.255.0
tacacs-server key goaway

radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization blue1
 ppp accounting red1

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

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 **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins”, which specifies that first RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network blue1 group radius local** command defines the network authorization method list named “blue1”, which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed.
- The **aaa accounting network red1 start-stop group radius group tacacs+** command defines the network accounting method list named red1, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using PPP. If the RADIUS server fails to respond, accounting services are handled by a TACACS+ server.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.

- The **tacacs-server host** command defines the name of the TACACS+ server host.
- The **tacacs-server key** command defines the shared secret text string between the network access server and the TACACS+ server host.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server 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 **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication chap dialins** command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.
- The **ppp authorization blue1** command applies the blue1 network authorization method list to the specified interfaces.
- The **ppp accounting red1** command applies the red1 network accounting method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- 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 only accept incoming calls.

The **show accounting** command yields the following output for the preceding configuration:

```
Active Accounted actions on tty1, User username2 Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
task_id=5 service=ppp protocol=ip address=10.0.0.98
```

Table 14 describes the fields contained in the preceding output.

Table 14 *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 Resource Accounting

The following example shows how to configure the resource failure stop accounting and resource accounting for start-stop records functions:

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method
to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to
use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

Example: Configuring AAA Broadcast Accounting

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

```
aaa group server radius isp
server 10.0.0.1
server 10.0.0.2

aaa group server tacacs+ isp_customer
server 172.0.0.1

aaa accounting network default start-stop broadcast group isp group isp_customer

radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

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:

```

aaa group server radius isp
  server 10.0.0.1
  server 10.0.0.2

aaa group server tacacs+ isp_customer
  server 172.0.0.1

aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer

radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2

```

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`.

Example: AAA Session MIB

The following example shows how to set up the AAA session MIB feature to disconnect authenticated client connections for PPP users:

```

aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect

```

Example: Configuring VRRS Accounting

The following example shows how to configure VRRS to send AAA Accounting messages to the AAA server:

```

Router# configure terminal
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay 10
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-group-1
Router(config-vrrs)# accounting delay 10
Router(config-vrrs)# accounting method vrrp-mlist-1
Router(config-vrrs)# exit

```


Additional References

Related Documents

Related Topic	Document Title
Authorization	“Configuring Authorization” module
Authentication	“Configuring Authentication” module
Accounting Commands	<i>Cisco IOS Security Command Reference</i>

Standards

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

MIBs

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

RFCs

RFC	Title
<i>RFC 2903</i>	<i>Generic AAA Architecture</i>
<i>RFC 2904</i>	<i>AAA Authorization Framework</i>
<i>RFC 2906</i>	<i>AAA Authorization Requirements</i>
<i>RFC 2989</i>	<i>Criteria for Evaluating AAA Protocols for Network Access</i>

Technical Assistance

Description	Link
<p>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for Configuring Accounting

Table 15 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 15 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 15 Feature Information for Configuring Accounting

Feature Name	Releases	Feature Information
AAA Broadcast Accounting	12.2 12.2S 12.2SB 12.2SX 12.4T	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. The following sections provide information about this feature: <ul style="list-style-type: none"> • AAA Broadcast Accounting, page 16 • Configuring AAA Broadcast Accounting, page 24
AAA Resource Accounting for Start-Stop Records	12.2 12.4T 12.2S 12.2SB 12.2SX	AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records. The following sections provide information about this feature: <ul style="list-style-type: none"> • AAA Resource Accounting for Start-Stop Records, page 15 • Configuring AAA Resource Accounting for Start-Stop Records, page 23

Table 15 Feature Information for Configuring Accounting

Feature Name	Releases	Feature Information
AAA Session MIB	12.2 12.4T 12.2S 12.2SB 12.2SX	<p>The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using 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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • AAA Session MIB, page 17 • Configuring AAA Session MIB, page 24
AAA: IPv6 Accounting Delay Enhancements	15.1(1)S	<p>VRRS provides a multienterprise information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • VRRS Accounting, page 15 • Configuring VRRS Accounting, page 26

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 1998–2010 Cisco Systems, Inc. All rights reserved.