



Configuring Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method you have 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/or auditing.

For a complete description of the accounting commands used in this chapter, refer to the “Accounting Commands” chapter in the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

In This Chapter

This chapter has the following sections:

- Named Method Lists for Accounting
- AAA Accounting Types
- AAA Accounting Prerequisites
- AAA Accounting Configuration Task List
- Accounting Attribute-Value Pairs
- Accounting Configuration Example

Named Method Lists for Accounting

Like authentication and authorization method lists, method lists for accounting define the way accounting will be performed and the sequence in which these methods are performed.

Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for accounting services. The only exception is the default method list (which, by coincidence, 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 enable you to designate one or more security protocols to be 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 five 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.

**Note**

System accounting does not use named accounting lists; you can only define the default list for system accounting.

Once again, when you create a named method list, you are defining a particular list of accounting methods for the indicated accounting type.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods will be 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 a named method list specified, 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.

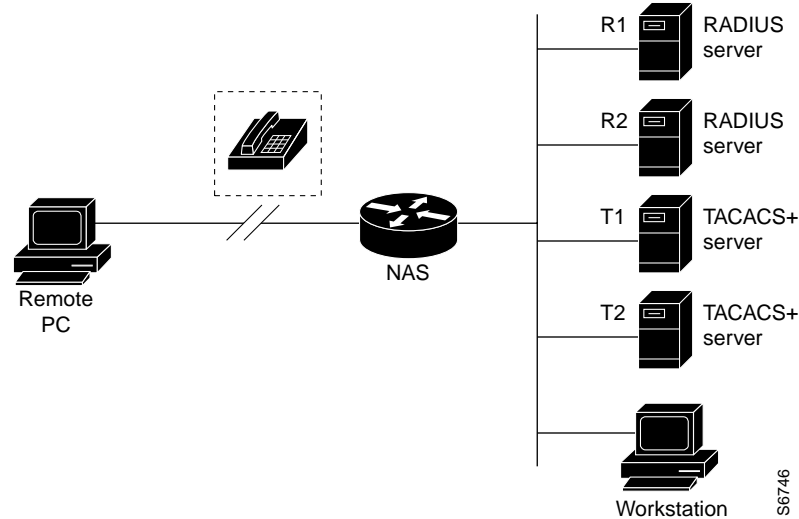
This section includes the following sections:

- Method Lists and Server Groups
- AAA Accounting Methods

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 6 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 6 Typical AAA Network Configuration



Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as separate server groups, and T1 and T2 as separate server groups. This means you can specify either R1 and T1 in the method list or R2 and T2 in the method list, which provides more flexibility in the way that you assign RADIUS and TACACS+ resources.

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 at 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 fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

For more information about configuring server groups and about configuring server groups based on DNIS numbers, refer to the “Configuring RADIUS” or “Configuring TACACS+” chapter.

AAA Accounting Methods

Cisco IOS 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 attribute-value (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 attribute-value (AV) pairs and is stored on the security server.

AAA Accounting Types

AAA supports five different accounting types:

- Network Accounting
- Connection Accounting
- EXEC Accounting
- System Accounting
- Command Accounting

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 25 04:44:45 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 5
  User-Name = "fgeorge"
  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 = "fgeorge"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 25 04:45:00 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 5
  User-Name = "fgeorge"
  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 = "fgeorge"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 25 04:47:46 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 5
  User-Name = "fgeorge"
  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 = "fgeorge"
NAS-Identifier = "172.16.25.15"

Wed Jun 25 04:48:45 1999
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "fgeorge"
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 = "fgeorge"
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 25 04:00:35 1999      172.16.25.15  fgeorge  tty4  562/4327528
starttask_id=28      service=shell
Wed Jun 25 04:00:46 1999      172.16.25.15  fgeorge  tty4  562/4327528
starttask_id=30      addr=10.1.1.1  service=ppp
Wed Jun 25 04:00:49 1999      172.16.25.15  fgeorge  tty4  408/4327528  update
task_id=30      addr=10.1.1.1  service=ppp  protocol=ip  addr=10.1.1.1
Wed Jun 25 04:01:31 1999      172.16.25.15  fgeorge  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 25 04:01:32 1999      172.16.25.15  fgeorge  tty4  562/4327528
stoptask_id=28      service=shell  elapsed_time=57

```


Note

The precise format of accounting packets records may vary depending on your particular 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 25 04:30:52 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 3
  User-Name = "fgeorge"
  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 = "fgeorge"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 25 04:36:49 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 3
  User-Name = "fgeorge"
  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 = "fgeorge"
  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 25 04:02:19 1999      172.16.25.15   fgeorge   Async5   562/4327528
starttask_id=35      service=ppp
Wed Jun 25 04:02:25 1999      172.16.25.15   fgeorge   Async5   562/4327528   update
task_id=35      service=ppp      protocol=ip      addr=10.1.1.2
Wed Jun 25 04:05:03 1999      172.16.25.15   fgeorge   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
```

Connection Accounting

Connection accounting 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.

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

```

Wed Jun 25 04:28:00 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 2
  User-Name = "fgeorge"
  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 = "171.68.202.158"
  Acct-Delay-Time = 0
  User-Id = "fgeorge"
  NAS-Identifier = "172.16.25.15"

Wed Jun 25 04:28:39 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 2
  User-Name = "fgeorge"
  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 = "171.68.202.158"
  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 = "fgeorge"
  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 25 03:47:43 1999      172.16.25.15      fgeorge  tty3      5622329430/4327528
start  task_id=10      service=connection      protocol=telnet addr=171.68.202.158
cmd=telnet fgeorge-sun
Wed Jun 25 03:48:38 1999      172.16.25.15      fgeorge  tty3      5622329430/4327528 stop
task_id=10      service=connection      protocol=telnet addr=171.68.202.158 cmd=telnet
fgeorge-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 25 04:29:48 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 2
  User-Name = "fgeorge"
  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 = "171.68.202.158"
  Acct-Delay-Time = 0
  User-Id = "fgeorge"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 25 04:30:09 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 2
  User-Name = "fgeorge"
  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 = "171.68.202.158"
  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 = "fgeorge"
  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 25 03:48:46 1999      172.16.25.15      fgeorge  tty3      5622329430/4327528
start   task_id=12      service=connection      protocol=rlogin addr=171.68.202.158
cmd=rlogin fgeorge-sun /user fgeorge
Wed Jun 25 03:51:37 1999      172.16.25.15      fgeorge  tty3      5622329430/4327528 stop
task_id=12      service=connection      protocol=rlogin addr=171.68.202.158 cmd=rlogin
fgeorge-sun /user fgeorge 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 25 03:53:06 1999      172.16.25.15      fgeorge  tty3      5622329430/4327528
start   task_id=18      service=connection      protocol=lat      addr=VAX      cmd=lat
VAX
Wed Jun 25 03:54:15 1999      172.16.25.15      fgeorge  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
```

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 25 04:26:23 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 1
  User-Name = "fgeorge"
  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 = "fgeorge"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 25 04:27:25 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 1
  User-Name = "fgeorge"
  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 = "fgeorge"
  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 25 03:46:21 1999      172.16.25.15  fgeorge  tty3  5622329430/4327528
start  task_id=2      service=shell
Wed Jun 25 04:08:55 1999      172.16.25.15  fgeorge  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 25 04:48:32 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 26
  User-Name = "fgeorge"
  Caller-ID = "171.68.202.158"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000010"
  Acct-Delay-Time = 0
  User-Id = "fgeorge"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 25 04:48:46 1999
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 26
  User-Name = "fgeorge"
  Caller-ID = "171.68.202.158"
  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 = "fgeorge"
  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 25 04:06:53 1999      172.16.25.15   fgeorge   tty26   171.68.202.158
starttask_id=41      service=shell
Wed Jun 25 04:07:02 1999      172.16.25.15   fgeorge   tty26   171.68.202.158
stoptask_id=41      service=shell   elapsed_time=9
```

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 25 03:55:32 1999      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 your particular TACACS+ daemon.

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

```
Wed Jun 25 03:55:22 1999      172.16.25.15   unknown unknown unknown stop    task_id=23
service=system event=sys_acct reason=reconfigure
```

**Note**

Cisco's implementation of RADIUS does not support system accounting.

Additional tasks for measuring system resources are covered in other chapters in the Cisco IOS software configuration guides. For example, IP accounting tasks are described in the “Configuring IP Services” chapter in the *Cisco IOS IP and IP Routing Configuration Guide*.

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 25 03:46:47 1999      172.16.25.15    fgeorge  tty3    5622329430/4327528  stop
task_id=3      service=shell  priv-lvl=1      cmd=show version <cr>
Wed Jun 25 03:46:58 1999      172.16.25.15    fgeorge  tty3    5622329430/4327528  stop
task_id=4      service=shell  priv-lvl=1      cmd=show interfaces Ethernet 0 <cr>
Wed Jun 25 03:47:03 1999      172.16.25.15    fgeorge  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 25 03:47:17 1999      172.16.25.15    fgeorge  tty3    5622329430/4327528  stop
task_id=6      service=shell  priv-lvl=15     cmd=configure terminal <cr>
Wed Jun 25 03:47:21 1999      172.16.25.15    fgeorge  tty3    5622329430/4327528  stop
task_id=7      service=shell  priv-lvl=15     cmd=interface Serial 0 <cr>
Wed Jun 25 03:47:29 1999      172.16.25.15    fgeorge  tty3    5622329430/4327528  stop
task_id=8      service=shell  priv-lvl=15     cmd=ip address 1.1.1.1 255.255.255.0 <cr>
```

**Note**

Cisco's implementation of RADIUS does not support command accounting.

AAA Accounting Prerequisites

Before configuring accounting using named method lists, you must first perform the following tasks:

- Enable AAA on your network access server. For more information about enabling AAA on your Cisco router or access server, refer to the “AAA Overview” chapter.
- Define the characteristics of your RADIUS or TACACS+ security server if you are issuing RADIUS or TACACS+ authorization. For more information about configuring your Cisco network access server to communicate with your RADIUS security server, refer to the “Configuring RADIUS” chapter. For more information about configuring your Cisco network access server to communicate with your TACACS+ security server, refer to the “Configuring TACACS+” chapter.

AAA Accounting Configuration Task List

This section describes the following configuration tasks:

- Configuring AAA Accounting Using Named Method Lists
- Suppressing Generation of Accounting Records for Null Username Sessions
- Generating Interim Accounting Records
- Suppressing Generation of Accounting Records for Failed Login or Session
- Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records
- Monitoring Accounting

For accounting configuration examples using the commands in this chapter, refer to the “Accounting Configuration Example” section at the end of the this chapter.

Configuring AAA Accounting Using Named Method Lists

To configure AAA accounting using named method lists, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [method1 [method2...]]</code>	Creates an accounting method list and enables accounting. The keyword <i>list-name</i> is a character string used to name the list you are creating.
Step 2	<code>line [aux console tty vty] line-number [ending-line-number]</code> or <code>interface interface-type interface-number</code>	Enters the line configuration mode for the lines to which you want to apply the accounting method list. or Enters the interface configuration mode for the interfaces to which you want to apply the accounting method list.
Step 3	<code>accounting {arap commands level connection exec} {default list-name}</code> or <code>ppp accounting {default list-name}</code>	Applies the accounting method list to a line or set of lines. or Applies the accounting method list to an interface or set of interfaces.



Note

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

This section includes the following sections:

- Accounting Types
- Accounting Record Types
- Accounting Methods

Accounting Types

Named accounting method lists are specific to the indicated type of accounting.

- **network**—To create a method list to enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARA protocols), use the **network** keyword. For example, to create a method list that provides accounting information for ARAP (network) sessions, use the **arap** keyword.
- **exec**—To create a method list that provides accounting records about user EXEC terminal sessions on the network access server, including username, date, start and stop times, use the **exec** keyword.
- **commands**—To create a method list that provides accounting information about specific, individual EXEC commands associated with a specific privilege level, use the **commands** keyword.
- **connection**—To create a method list that provides accounting information about all outbound connections made from the network access server, use the **connection** keyword.



Note

System accounting does not support named method lists.

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 10 lists the supported accounting methods.

Table 10 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 you want 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. For more specific information about configuring TACACS+ for accounting services, refer to the “Configuring TACACS+” chapter.
- **group radius**—To have the network access server send accounting information to a RADIUS security server, use the **group radius method** keyword. For more specific information about configuring RADIUS for accounting services, refer to the “Configuring RADIUS” chapter.



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 you can use a group name as the accounting method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the “Configuring RADIUS” chapter. For more information about establishing communication with a TACACS+ server, refer to the “Configuring TACACS+” chapter.

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
<code>aaa accounting suppress null-username</code>	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
<code>aaa accounting update {[newinfo] [periodic] number}</code>	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 will be 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 will include 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 argument number. 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.

Suppressing Generation of 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
<code>aaa accounting send stop-record authentication failure</code>	Generates stop-records for users who fail to authenticate at login or during session negotiation using PPP.

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, you can specify that NETWORK records be generated before EXEC-stop records. In some 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
<code>aaa accounting nested</code>	Nests network accounting records.

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
<code>show accounting</code>	Steps through all active sessions and print all the accounting records for the actively accounted functions.

Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ attribute-value (AV) pairs or RADIUS attributes, depending on which security method you have implemented. For a list of supported RADIUS accounting attributes, refer to the “RADIUS Attributes” appendix. For a list of supported TACACS+ accounting AV pairs, refer to the “TACACS+ AV Pairs” appendix.

Accounting Configuration Example

This section contains the Named Method List Configuration Example.

Named Method List Configuration Example

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database will be queried for authentication and authorization information, and accounting services will be handled by a TACACS+ server.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network scoobee group radius local
aaa accounting network charley 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 scoobee
 ppp accounting charley

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 RADIUS authentication then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network scoobee group radius local** command defines the network authorization method list named scoobee, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization will be performed.
- The **aaa accounting network charley start-stop group radius group tacacs+** command defines the network accounting method list named charley, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) will be used on serial lines using PPP. If the RADIUS server fails to respond, accounting services will be 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 scoobee** command applies the scoobee network authorization method list to the specified interfaces.
- The **ppp accounting charley** command applies the charley 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 rubble 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 11 describes the fields contained in the preceding output.

Table 11 *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.