



Implementing Server-Based AAA Accounting

This chapter focuses on the following two topics:

- 5.1 Implementing Server-Based RADIUS Dial Accounting
- 5.2 Implementing Server-Based TACACS+ Router Accounting



Caution

The example configuration fragments used throughout this chapter include IP addresses, passwords, authentication keys, and other variables that are specific to this case study. If you use these fragments as foundations for your own configurations, be sure that your specifications apply to your environment.



Note

See “1.1 AAA Technology Summary,” in Chapter 1 for brief definitions of authentication, authorization, and accounting as they relate to AAA security implementation.

5.1 Implementing Server-Based RADIUS Dial Accounting

The information compiled by the Cisco IOS client focuses on the performance of intermediate systems in terms of AAA accounting packet output, disconnect cause codes, elapsed time, packets in/out, and other useful information. This section addresses configuring server-based RADIUS dial accounting on the AAA server and the Cisco IOS client or network access server (NAS).

These steps help you to accomplish the following tasks:

1. Configure the server-based RADIUS dial accounting on the AAA server.
2. Configure server-based RADIUS dial accounting on the NAS.
3. Verify and troubleshoot server-based accounting from the AAA server by using an SQL query to Oracle dB instance.
4. Verify AAA accounting from the NAS.

Step 1 Configure the server-based RADIUS dial accounting on the AAA server.

Include the following configuration line in `/opt/ciscosecure/CLI/config/CSU.cfg` to enable group membership accounting:

```
config_acct_fn_enable = 1
```

For detailed accounting performance, go to:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csu23ug/acctg.htm#xto cid84517

Step 2 Configure server-based RADIUS dial accounting on the NAS.

Include the following Cisco IOS commands in your configuration file to support dialup authentication, authorization, and accounting.

```
aaa new-model
aaa authentication login default group radius local
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius if-authenticated
aaa accounting exec default stop-only group radius
aaa accounting network default stop-only group radius
```

Step 3 Verify and troubleshoot server-based accounting from the AAA server by using an SQL query to Oracle dB instance.

The following examples illustrate the use of SQL query commands to monitor user *rad_dial* being disconnected due to idletime configured with the line configuration **session-timeout** command in the NAS:

```
<CSUServer>$/export/home/oracle> sqlplus

SQL*Plus: Release 3.3.4.0.1 - Production on Mon Apr 17 17:41:52 2000

Copyright (c) Oracle Corporation 1979, 1996. All rights reserved.

Enter user-name:csecure/csecure@ciscoaus
Connected to:
Oracle7 Server Release 7.3.4.0.1 - Production
PL/SQL Release 2.3.4.0.0 - Production

SQL> select * from cs_accounting_log where blob_data like '%rad_dial%';

LOG_ID BLOB_ORDINAL BLOB_DATA
-----
172.22.87.3 rad_dial Async20 65004 stop server=danvers time=17:36:33
date=04/17/2000 task_id=40 timezone=CST service=ppp protocol=ip
addr=172.22.83.12 disc-cause=4 disc-cause-ext=1021 pre-bytes-in=132
pre-bytes-out=139 pre-paks-in=5 pre-paks-out=7 bytes_i
```



Note The **disc-cause** and **disc-cause-ext** output both reflect idle timeouts from Table 5-1 listed in “5.3 AAA Disconnect Cause Code Descriptions” in this chapter.

Step 4 Verify AAA accounting from the NAS.

Review and verify user *rad_dial* disconnecting session from the NAS by using the Cisco IOS **show caller user** and **debug aaa accounting** commands.

The following example illustrates local accounting diagnostic output in which user *rad_dial* is disconnected because of a line configuration **session-timeout** command configured in the NAS:



Note User *rad_dial* dials into *maui-nas-03*. Note the session-timeout was applied.

```
maui-nas-03#show caller user rad_dial detail

User: rad_dial, line tty 20, service Async
  Active time 00:00:47, Idle time 00:00:00
Timeouts:          Absolute  Idle      Idle
                  Session   Exec
  Limits:          04:00:00  00:15:00  00:48:00
  Disconnect in:   03:59:12  00:14:59  -
TTY: Line 20, running PPP on As20
Location: PPP: 172.22.83.12
DS0: (slot/unit/channel)=0/0/2
Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: Ready, Active, No Exit Banner, Async Interface Active
      HW PPP Support Active, Modem Detected
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
              Modem Callout, Modem RI is CD,
              Line usable as async interface, Modem Autoconfigure
              Integrated Modem
Modem State: Ready, Modem Configured

User: rad_dial, line As20, service PPP
  Active time 00:00:44, Idle time 00:00:08
Timeouts:          Absolute  Idle
  Limits:          -          00:15:00
  Disconnect in:     -          00:14:50
```

User *rad_dial* is disconnected after 15 minutes of inactivity and an accounting packet is sent to the AAA Server:

```
maui-nas-03#show debug
General OS:
  AAA Accounting debugging is on

*Apr 17 17:36:35.262 CST: AAA/ACCT/ACCT_DISC: Found list "default"
*Apr 17 17:36:35.262 CST: Async20 AAA/DISC: 4/"Idle Timeout"
*Apr 17 17:36:35.262 CST: AAA/ACCT/ACCT_DISC: Found list "default"
*Apr 17 17:36:35.262 CST: Async20 AAA/DISC/EXT: 1021/"Idle Timeout"
*Apr 17 17:36:35.262 CST: Async20 AAA/DISC: 4/"Idle Timeout"
*Apr 17 17:36:35.262 CST: Async20 AAA/DISC/EXT: 1021/"Idle Timeout"
```



Note The `disc-cause` and `disc-cause-ext` both reflect idle timeouts from Table 5-1 listed in “5.3 AAA Disconnect Cause Code Descriptions” in this chapter.

5.2 Implementing Server-Based TACACS+ Router Accounting

These steps help you to accomplish the following tasks:

1. Configure the server-based TACACS+ router accounting on the AAA server.
2. Configure server-based TACACS+ EXEC and command level accounting on the router.
3. Verify and troubleshoot server-based accounting from the AAA Server with SQL query to Oracle dB instance.
4. Verify and troubleshoot server-based accounting operation from the router.

Step 1 Configure the server-based TACACS+ router accounting on the AAA server.

config_acct_fn_enable = 1

For detailed accounting performance, go to:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csu23ug/acctg.htm#xto cid84517

Step 2 Configure server-based TACACS+ EXEC and command level accounting on the router.

Include the following Cisco IOS commands in your configuration file to enable router EXEC and command AAA authentication, authorization, and accounting:

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login NO_AUTHEN none
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 default group tacacs+
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+

line con 0
authorization commands 15 NO_AUTHOR
authorization exec NO_AUTHOR
login authentication NO_AUTHEN
```



Note Authentication and authorization is disabled on the console port with the use of the **NO_AUTHEN** and **NO_AUTHOR** named lists.

- Step 3** Verify and troubleshoot server-based accounting from the AAA Server with SQL query to Oracle dB instance.

The following example illustrates the use of the SQL query **select** command to monitor user *rtr_geek* entering the **configure terminal** privilege level 15 command:

```
SQL>select * from cs_accounting_log where blob_data like '%rtr_geek%';

LOG_ID BLOB_ORDINAL      BLOB_DATA
-----
Mon Apr 17 14:06:27 2000
  Client-Id = 172.22.80.3
  Client-Port-Id = 0
  NAS-Port-Type = Async
  User-Name = "rtr_geek"
  Acct-Status-Type = Stop

LOG_ID BLOB_ORDINAL      BLOB_DATA
-----
172.22.87.3      rtr_geek      tty0      async      stop      server=danvers      time=18:10:02
date=04/17/2000      task_id=52      timezone=CST      service=shell      priv-lvl=15
cmd=configure terminal <cr>
```

- Step 4** Verify and troubleshoot server-based accounting operation from the router.

Enter the **configure terminal** command to test AAA accounting behavior as follows (be sure the **debug aaa accounting** command is enabled):

```
maui-nas-03#show debug
General OS:
  AAA Accounting debugging is on
maui-nas-03#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
maui-nas-03(config)#^Z
```

This **debug** command output results from entering the **configure terminal** command:

```
*Apr 17 18:14:45.722 CST: AAA/ACCT/CMD: User rtr_geek, Port tty0, Priv 15:
  "configure terminal <cr>"
*Apr 17 18:14:45.722 CST: AAA/ACCT/CMD: Found list "default"
*Apr 17 18:14:45.726 CST: AAA/ACCT: user rtr_geek, acct type 3 (1057208544):
Method=tacacs+ (tacacs+)
*Apr 17 18:14:45.930 CST: TAC+: (1057208544): received acct response status = SUCCESS
```

5.3 AAA Disconnect Cause Code Descriptions

Table 5-1 lists the disconnect codes reported by Cisco AAA accounting records. The disconnect cause codes are referred to in “5.1 Implementing Server-Based RADIUS Dial Accounting.”

Table 5-1 AAA Disconnect Cause Code Listings

Disconnect Cause Code	Description
1	User Request
2	Lost Carrier
3	Lost Service
4	Idle Timeout
5	Session Timeout
6	Admin Reset
7	Admin Reboot
8	Port Error
9	NAS Error
10	NAS Request
11	NAS Reboot
12	Port Unneeded
13	Port Preempted
14	Port Suspended
15	Service Unavailable
16	Callback
17	User Error
18	Host Request
1002	Unknown
1004	CLID Auth Fail
1010	No Carrier
1011	AAA_VAL_DISC_LOST_CARR
1012	No Modem result codes
1020	AAA_VAL_DISC_USER_REQ
1021	AAA_VAL_DISC_IDL_TIMEOUT
1022	Exited Telnet
1023	Peer has No IPADDR
1024	AAA_VAL_DISC_LOST_SERV
1025	Password failure
1026	TCP Disabled
1027	Control-C Detected
1028	AAA_VAL_DISC_HOST_REQ

Table 5-1 AAA Disconnect Cause Code Listings

Disconnect Cause Code	Description
1040	LCP Neg Timeout
1041	LCP Neg Failed
1042	PAP Auth Failed
1043	CHAP Auth Failed
1044	Remote Auth Failed
1045	Received Terminate
1046	Upper Layer Req Close
1100	AAA_VAL_DISC_SES_TIMEOUT
1101	Fail Security
1102	AAA_VAL_DISC_CALLBACK
1120	AAA_VAL_DISC_SERV_UNAVAIL

