



Implementing the Local AAA Subsystem

This chapter focuses on *local* AAA implementation and describes the following topics:

- 2.1 Implementing Local Dialup Authentication
- 2.2 Implementing Local Dialup Authorization
- 2.3 Implementing Local Router Authentication
- 2.4 Implementing Local Router Authorization



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.

Server-based authentication, authorization, and accounting issues are described in the following chapters:

- Chapter 3, “Implementing Cisco AAA Servers”
- Chapter 4, “Implementing the Server-Based AAA Subsystem”
- Chapter 5, “Implementing Server-Based AAA Accounting”
- Chapter 6, “Diagnosing and Troubleshooting AAA Operations”



Caution

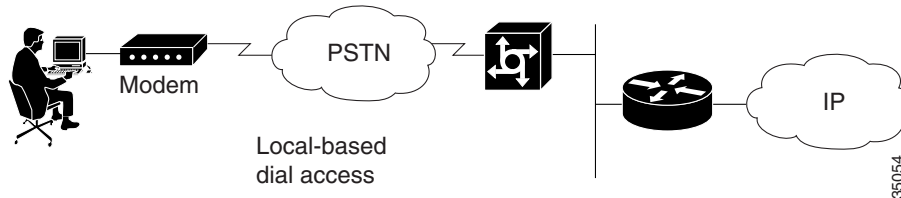
The example configuration fragments used throughout this chapter include IP addresses, passwords, authentication keys, and other variables that are specific to this case study. If you use these fragments as foundations for your own configurations, be sure that your specifications apply to your environment.

2.1 Implementing Local Dialup Authentication

These steps help you to establish local-based dial authentication as illustrated in Figure 2-1:

1. Configure basic dial access.
2. Verify basic dial access.

Figure 2-1 Local-Based Dial Access Environment



Step 1 Configure basic dial access.

Include the following Cisco IOS configuration commands in your configuration to construct dial access local authentication control:

```

aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
username diallocal password xxxxxx

interface Group-Async1
 ip unnumbered Loopback0
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 no logging event link-status
 dialer in-band
 dialer idle-timeout 900
 async mode interactive
 no snmp trap link-status
 peer default ip address pool default
 no fair-queue
 no cdp enable
 ppp max-bad-auth 3
 ppp authentication pap chap
 group-range 1 48

line 1 48
 exec-timeout 48 0
 autoselect during-login
 autoselect ppp
 absolute-timeout 240
 script dialer cisco_default
 modem InOut
 modem autoconfigure type mica
 transport preferred telnet
 transport input all
 transport output pad telnet rlogin udptn

```



Note See “A.3 NAS AAA Command Implementation Descriptions” in Appendix A, “AAA Device Configuration Listings” for notes regarding key Cisco IOS AAA commands.

Step 2 Verify basic dial access.

- a. To verify user access, initiate a login process as follows:

```
maui-nas-01#login
```

```
User Access Verification
```

```
Username: diallocal
```

```
Password: <password>
```

- b. To determine that local dial access authentication is operating correctly, enter the **debug aaa authentication** and **debug ppp authentication** commands.

The following **debug** output contains only pertinent information:

```
maui-nas-01#
```

```
Debugs in NAS then initiate dialup:
```

```
maui-nas-01#debug aaa authentication
```

```
AAA Authentication debugging is on
```

```
maui-nas-01#debug ppp authentication
```

```
PPP authentication debugging is on
```

```
maui-nas-01#show debug
```

```
General OS:
```

```
AAA Authentication debugging is on
```

```
PPP:
```

```
PPP authentication debugging is on
```

The following shell-initiated PPP session example shows the AAA debug output that confirms correct configuration for local authentication:



Note The method used is LOCAL.

```

113123: Feb  4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb  4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
action=LOGIN service=LOGIN
113125: Feb  4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb  4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb  4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb  4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='(undef)')
113129: Feb  4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb  4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb  4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb  4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='diallocal')
113133: Feb  4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb  4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb  4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
113136: Feb  4 10:11:32.582 CST: As1 PPP: Treating connection as a callin
113137: Feb  4 10:11:32.582 CST: AAA/MEMORY: dup_user (0x61DF306C) user='dialuser'
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=PPP priv=1
source='AAA dup lcp_reset'
113138: Feb  4 10:11:32.582 CST: As1 AAA/AUTHEN: Method=IF-NEEDED: no authentication
needed. user='diallocal' port='tty1' rem_addr='async/81560'
113139: Feb  4 10:11:32.582 CST: AAA/MEMORY: free_user (0x619C4940) user='dialuser'
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113140: Feb  4 10:11:33.158 CST: AAA/MEMORY: dup_user (0x6193A788) user='dialuser'
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=PPP priv=1
source='AAA dup lcp_reset'
113141: Feb  4 10:11:33.158 CST: AAA/MEMORY: free_user (0x61DF306C) user='dialuser'
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=PPP priv=1
113142: Feb  4 10:11:33.158 CST: As1 AAA/AUTHEN: Method=IF-NEEDED: no authentication
needed. user='diallocal' port='tty1' rem_addr='async/81560'

```

The following example of a non-shell-initiated PPP session shows AAA **debug** output that confirms correct configuration for local authentication:



Note The method used is LOCAL.

```

113151: Feb  4 10:13:27.670 CST: AAA/MEMORY: create_user (0x61DFE188) user=''
ruser='' port='tty2' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113152: Feb  4 10:13:27.670 CST: AAA/AUTHEN/START (776784700): port='tty2' list=''
action=LOGIN service=LOGIN
113153: Feb  4 10:13:27.670 CST: AAA/AUTHEN/START (776784700): using "default" list
113154: Feb  4 10:13:27.670 CST: AAA/AUTHEN/START (776784700): Method=LOCAL
113155: Feb  4 10:13:27.670 CST: AAA/AUTHEN (776784700): status = GETUSER
113156: Feb  4 10:13:27.710 CST: AAA/AUTHEN/ABORT: (776784700) because Autoselected.
113157: Feb  4 10:13:27.710 CST: AAA/MEMORY: free_user (0x61DFE188) user='' ruser=''
port='tty2' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113158: Feb  4 10:13:29.842 CST: As2 PPP: Treating connection as a callin
113159: Feb  4 10:13:34.834 CST: As2 PAP: I AUTH-REQ id 1 len 18 from "diallocal"
113160: Feb  4 10:13:34.834 CST: As2 PAP: Authenticating peer diallocal
113161: Feb  4 10:13:34.838 CST: AAA: parse name=Async2 idb type=10 tty=2
113162: Feb  4 10:13:34.838 CST: AAA: name=Async2 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=2 channel=0
113163: Feb  4 10:13:34.838 CST: AAA: parse name=Serial0:3 idb type=12 tty=-1
113164: Feb  4 10:13:34.838 CST: AAA: name=Serial0:3 flags=0x51 type=1 shelf=0 slot=0
adapter=0 port=0 channel=3
113165: Feb  4 10:13:34.838 CST: AAA/MEMORY: create_user (0x61ABBCE4) user='dialuser'
ruser='' port='Async2' rem_addr='async/81560' authen_type=PAP service=PPP priv=1
113166: Feb  4 10:13:34.838 CST: AAA/AUTHEN/START (1001880850): port='Async2' list=''
action=LOGIN service=PPP
113167: Feb  4 10:13:34.838 CST: AAA/AUTHEN/START (1001880850): using "default" list
113168: Feb  4 10:13:34.838 CST: AAA/AUTHEN (1001880850): status = UNKNOWN
113169: Feb  4 10:13:34.838 CST: AAA/AUTHEN/START (1001880850): Method=LOCAL
113170: Feb  4 10:13:34.838 CST: AAA/AUTHEN (1001880850): status = PASS
113171: Feb  4 10:13:34.838 CST: As2 PAP: O AUTH-ACK id 1 len 5

```

2.2 Implementing Local Dialup Authorization

These processes help you to accomplish the following tasks:

1. Configure dial access configuration for local authorization on the NAS.
2. Verify and troubleshoot local authorization from NAS.
3. Verify that access list 110 is assigned.



Note Attribute-value pairs (AVPs) only are supported with EXEC shell initiated PPP sessions for local accounts. Configure dial access clients to “Bring Up a Terminal Window After Dial”.

Step 1 Configure dial access configuration for local authorization on the NAS.

Include the following Cisco IOS configuration commands in your configuration to construct dial access local authorization:

```
aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
aaa authorization exec default local if-authenticated
aaa authorization network default local if-authenticated

username dialclient access-class 110 password ciscorocks
username dialclient autocommand ppp negotiate

access-list 110 deny tcp any any eq telnet
access-list 110 permit tcp any any
```



Note See “A.3 NAS AAA Command Implementation Descriptions” in Appendix A, “AAA Device Configuration Listings” for notes regarding key Cisco IOS AAA commands.

Step 2 Verify and troubleshoot local authorization from NAS.

To verify local dial access authorization is operating correctly, enter the **debug aaa authorization** command.

The following EXEC sequence illustrates that the appropriate command is enabled:

```
5800-NAS#show debug
General OS:
  AAA Authorization debugging is on
```

The following example of a shell-initiated session shows the AAA **debug** output that confirms correct configuration for local authorization. Some points to note about this **debug** output:

- Method used is LOCAL.
- Autocommand used is PPP negotiate.
- Access list used is 110.
- Authorization is successful.

The following tests illustrate operations described in “2.4 Implementing Local Router Authorization” and include relevant router output:

1. User diallocal is authorized EXEC Shell Service (Terminal Window After Dial enabled).
2. EXEC Authorization in action; access-list 110 and autocommand=ppp negototiate AVPs processed.
3. User diallocal is authorized PPP Network Service.
4. User diallocal is authorized LCP.
5. User diallocal is authorized IPCP.

The following diagnostic results are presented in the order in which they are generated during the authorization process. Specific output fragments are differentiated with brief explanatory notes to help you identify relevant information.



Note The **debug** command output can vary depending on Cisco IOS versions.

1. User *diallocal* is authorized EXEC Shell Service (Terminal Window After Dial enabled).

NAS **debug** output:

```
07:10:52: As10 AAA/AUTHOR/EXEC (693880654): Port='tty10' list='' service=EXEC
07:10:52: AAA/AUTHOR/EXEC: As10 (693880654) user='diallocal'
07:10:52: As10 AAA/AUTHOR/EXEC (693880654): send AV service=shell
07:10:52: As10 AAA/AUTHOR/EXEC (693880654): send AV cmd*
07:10:52: As10 AAA/AUTHOR/EXEC (693880654): found list "default"
07:10:52: As10 AAA/AUTHOR/EXEC (693880654): Method=LOCAL
07:10:52: As10 AAA/AUTHOR (693880654): Post authorization status = PASS_ADD
```

2. EXEC Authorization in action; access-list 110 and autocommand=ppp negotiate AVPs processed.

NAS **debug** output:

```
07:10:52: AAA/AUTHOR/EXEC: Processing AV service=shell
07:10:52: AAA/AUTHOR/EXEC: Processing AV cmd*
07:10:52: AAA/AUTHOR/EXEC: Processing AV autocmd=ppp
07:10:52: AAA/AUTHOR/EXEC: Processing AV acl=110
07:10:52: AAA/AUTHOR/EXEC: Authorization successful
```

3. User *diallocal* is authorized PPP Network Service.

NAS **debug** output:

```
07:10:52: As10 AAA/AUTHOR/PPP (2856468577): Port='tty10' list='' service=NET
07:10:52: AAA/AUTHOR/PPP: As10 (2856468577) user='diallocal'
07:10:52: As10 AAA/AUTHOR/PPP (2856468577): send AV service=ppp
07:10:52: As10 AAA/AUTHOR/PPP (2856468577): send AV protocol=ip
07:10:52: As10 AAA/AUTHOR/PPP (2856468577): send AV addr-pool*default
07:10:52: As10 AAA/AUTHOR/PPP (2856468577): found list "default"
07:10:52: As10 AAA/AUTHOR/PPP (2856468577): Method=LOCAL
07:10:52: As10 AAA/AUTHOR (2856468577): Post authorization status = PASS_REPL
```

4. User *diallocal* is authorized LCP.

NAS **debug** output:

```
07:10:52: AAA/AUTHOR/Async10: PPP: Processing AV service=ppp
07:10:52: AAA/AUTHOR/Async10: PPP: Processing AV protocol=ip
07:10:52: AAA/AUTHOR/Async10: PPP: Processing AV addr-pool*default
07:10:54: AAA/MEMORY: free_user (0x61851148) user='diallocal' ruser='' port='tty
10' rem_addr='65004/65301' authen_type=ASCII service=LOGIN priv=1
07:10:56: AAA/MEMORY: free_user (0x61532710) user='diallocal' ruser='' port='tty
10' rem_addr='65004/65301' authen_type=ASCII service=PPP priv=1
07:10:56: As10 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
07:10:58: As10 AAA/AUTHOR/LCP: Authorize LCP
07:10:58: As10 AAA/AUTHOR/LCP (3185006257): Port='tty10' list='' service=NET
07:10:58: AAA/AUTHOR/LCP: As10 (3185006257) user='diallocal'
07:10:58: As10 AAA/AUTHOR/LCP (3185006257): send AV service=ppp
07:10:58: As10 AAA/AUTHOR/LCP (3185006257): send AV protocol=lcp
07:10:58: As10 AAA/AUTHOR/LCP (3185006257): found list "default"
07:10:58: As10 AAA/AUTHOR/LCP (3185006257): Method=LOCAL
07:10:58: As10 AAA/AUTHOR (3185006257): Post authorization status = PASS_REPL
```

5. User *diallocal* is authorized IPCP.

NAS debug output:

```
07:10:58: As10 AAA/AUTHOR/LCP: Processing AV service=ppp
07:10:58: As10 AAA/AUTHOR/LCP: Processing AV protocol=lcp
07:10:58: As10 AAA/AUTHOR/FSM (321297806): Port='tty10' list='' service=NET
07:10:58: AAA/AUTHOR/FSM: As10 (321297806) user='diallocal'
07:10:58: As10 AAA/AUTHOR/FSM (321297806): send AV service=ppp
07:10:58: As10 AAA/AUTHOR/FSM (321297806): send AV protocol=ip
07:10:58: As10 AAA/AUTHOR/FSM (321297806): found list "default"
07:10:58: As10 AAA/AUTHOR/FSM (321297806): Method=LOCAL

07:10:58: As10 AAA/AUTHOR (321297806): Post authorization status = PASS_REPL
07:10:58: As10 AAA/AUTHOR/FSM: We can start IPCP
```

- Step 3** Verify that access list 110 is assigned.

To verify that access list 110 is being used to control access, enter the **show line** command as follows:

```
maui-nas-03#show line 10
  Tty Typ   Tx/Rx   A Modem  Roty AccO AccI   Uses  Noise  Overruns  Int
A   10 TTY             - inout   -  110   -     1     0     0/0     -
```



Note

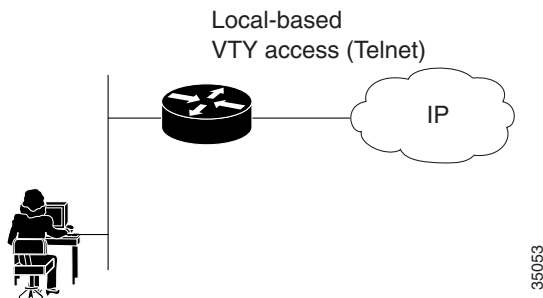
Access lists can be defined as either input or output access lists. As configured and applied in this environment, access list 110 is an output access list assigned with the `ac1=110` AVP. In the **show line** listing, `AccO` refers to output access list 110. In this case, `AccI` is not set (indicated by a dash).

2.3 Implementing Local Router Authentication

These processes help you to establish local-based router authentication as illustrated in Figure 2-2:

1. Configure basic router access.
2. Verify local authentication operation.

Figure 2-2 Local-Based Router Environment



Step 1 Configure basic router access.

Include the following Cisco IOS configuration commands in your configuration to enforce *local* on all interfaces except the console port:

```
username rtr_super privilege 15 password ciscorules
!
aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHENT none
!
line con 0
  login authentication NO_AUTHENT
```



Note The NO_AUTHENT list disables authentication on the console port. See “A.2 Router AAA Command Implementation Descriptions” in Appendix A, “AAA Device Configuration Listings” for notes regarding Cisco IOS AAA commands.

Step 2 Verify local authentication operation.

- a. To verify user access, initiate a login process as follows:

```
maui-rtr-03#login

User Access Verification

Username: rtr_super
Password: <password>

maui-rtr-03#
```

- b. To determine that local dial access authentication is operating correctly, enter the **debug aaa authentication** command as follows:

```

maui-rtr-03#debug aaa authentication
AAA Authentication debugging is on
maui-rtr-03#show debug
General OS:
  AAA Authentication debugging is on

maui-rtr-03#terminal monitor

Feb 17 15:34:47.147: AAA: parse name=tty3 idb type=-1 tty=-1
Feb 17 15:34:47.147: AAA: name=tty3 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=3
channel=0
Feb 17 15:34:47.147: AAA/MEMORY: create_user (0x61F88D2C) user='' ruser=''
port='tty3' rem_addr='172.22.61.17' authen_type=ASCII service=LOGIN priv=1
Feb 17 15:34:47.147: AAA/AUTHEN/START (3701879404): port='tty3' list='' action=LOGIN
service=LOGIN
Feb 17 15:34:47.147: AAA/AUTHEN/START (3701879404): using "default" list
Feb 17 15:34:47.147: AAA/AUTHEN/START (3701879404): Method=LOCAL
Feb 17 15:34:47.147: AAA/AUTHEN (3701879404): status = GETUSER
Feb 17 15:34:49.679: AAA/AUTHEN/CONT (3701879404): continue_login (user='(undef)')
Feb 17 15:34:49.679: AAA/AUTHEN (3701879404): status = GETUSER
Feb 17 15:34:49.679: AAA/AUTHEN/CONT (3701879404): Method=LOCAL
Feb 17 15:34:49.679: AAA/AUTHEN (3701879404): status = GETPASS
Feb 17 15:34:51.467: AAA/AUTHEN/CONT (3701879404): continue_login (user='rtr_super')
Feb 17 15:34:51.467: AAA/AUTHEN (3701879404): status = GETPASS
Feb 17 15:34:51.467: AAA/AUTHEN/CONT (3701879404): Method=LOCAL
Feb 17 15:34:51.467: AAA/AUTHEN (3701879404): status = PASS

```

2.4 Implementing Local Router Authorization

Local router authorization is implemented through router command authorization configuration. The following example:

- Shows how to create two *privilege levels* (1 and 15) with local access and how to control the access to global configuration mode.
- Provides a method to gain access by using the enable password if the local login fails.

Follow a methodical approach when dealing with TACACS+ in routers to prevent the need to perform password recovery.



Note Some versions of boot ROMs do not recognize all AAA commands. Be sure to disable AAA authentication and authorization before changing to boot ROM mode. For configuration notes regarding disabling AAA to access boot ROM mode, see Appendix B, “AAA Impact on Maintenance Tasks.”

These processes are intended to help you to accomplish the following tasks:

1. Configure local router authorization at privilege level 15.
2. Verify local router authorization is set to privilege level 15.

Step 1 Configure local router authorization at privilege level 15.

Include the following Cisco IOS configuration commands in your configuration to enforce local authorization at privilege level 15 on all interfaces except the console port:

```
!
username rtr_super privilege 15 password ciscorules
!
aaa new-model
aaa authentication login default local enable
aaa authentication login NO_AUTHENT none
aaa authorization exec default local if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 NO_AUTHOR none
aaa authorization commands 15 local if-authenticated
!
line con 0
  authorization commands 15 NO_AUTHOR
  authorization exec NO_AUTHOR
  login authentication NO_AUTHENT
```



Note You must first log out, and then log back into the router following the inclusion of the **aaa authorization commands 15 local if-authenticated** command (illustrated in the preceding configuration fragment). Doing this ensures that you log in as the user *rtr_super* (in this case study example). The **NO_AUTHENT** list disables authentication on the console port. The **NO_AUTHOR** list disables EXEC and command authorization on the console port. See “A.2 Router AAA Command Implementation Descriptions” in Appendix A, “AAA Device Configuration Listings” for notes regarding key Cisco IOS AAA commands.

Step 2 Verify local router authorization is set to privilege level 15.

Enter the following commands to verify correct authorization:

```
maui-rtr-03#debug aaa authorization
AAA Authorization debugging is on
maui-rtr-03#show debug
General OS:
  AAA Authorization debugging is on
```

```
maui-rtr-03#login
```

```
User Access Verification
```

```
Username: rtr_super
Password:
```

The following tests illustrate operations described in “2.4 Implementing Local Router Authorization” and include relevant router output.

1. User *rtr_super* is authorized EXEC shell access.
2. User *rtr_super* logs in assigned priv-lvl 15 AVP.
3. User *rtr_super* successfully performs privilege level 15 command.

The following diagnostic results are presented in the order in which they are generated during the authorization process. Specific output fragments are differentiated with brief explanatory notes to help you identify relevant information.



Note The **debug** command output can vary depending on Cisco IOS versions.

1. User *rtr_super* is authorized EXEC shell access.

Router **debug** output:

```
Mar 13 14:08:54.871 CST: AAA/MEMORY: create_user (0x6188BD2C) user='' ruser=''
port='tty2' rem_addr='172.22.53.201' authen_type=ASCII service=LOGIN priv=15
Mar 13 14:09:00.511 CST: tty2 AAA/AUTHOR/EXEC (294199586): Port='tty2' list=''
service=EXEC
Mar 13 14:09:00.511 CST: AAA/AUTHOR/EXEC: tty2 (294199586) user='rtr_super'
Mar 13 14:09:00.511 CST: tty2 AAA/AUTHOR/EXEC (294199586): send AV service=shell
Mar 13 14:09:00.511 CST: tty2 AAA/AUTHOR/EXEC (294199586): send AV cmd*
Mar 13 14:09:00.511 CST: tty2 AAA/AUTHOR/EXEC (294199586): found list "default"
Mar 13 14:09:00.511 CST: tty2 AAA/AUTHOR/EXEC (294199586): Method=LOCAL
Mar 13 14:09:00.511 CST: AAA/AUTHOR (294199586): Post authorization status = PASS_ADD
```

2. User *rtr_super* logs is assigned priv-lvl 15 AVP.

Router **debug** output:

```
Mar 13 14:09:00.511 CST: AAA/AUTHOR/EXEC: Processing AV service=shell
Mar 13 14:09:00.511 CST: AAA/AUTHOR/EXEC: Processing AV cmd*
Mar 13 14:09:00.511 CST: AAA/AUTHOR/EXEC: Processing AV priv-lvl=15
Mar 13 14:09:00.511 CST: AAA/AUTHOR/EXEC: Authorization successful
Mar 13 14:09:01.648 CST: tty2 AAA/AUTHOR/CMD (2192867088): Port='tty2' list=''
service=CMD
```

3. User *rtr_super* successfully performs privilege level 15 command.

Router **debug** output:

```
Mar 13 14:09:01.648 CST: AAA/AUTHOR/CMD: tty2 (2192867088) user='rtr_super'
Mar 13 14:09:01.648 CST: tty2 AAA/AUTHOR/CMD (2192867088): send AV service=shell
Mar 13 14:09:01.648 CST: tty2 AAA/AUTHOR/CMD (2192867088): send AV cmd=configure
Mar 13 14:09:01.648 CST: tty2 AAA/AUTHOR/CMD (2192867088): send AV cmd-arg=terminal
Mar 13 14:09:01.648 CST: tty2 AAA/AUTHOR/CMD (2192867088): send AV cmd-arg=<cr>
Mar 13 14:09:01.648 CST: tty2 AAA/AUTHOR/CMD (2192867088): found list "default"
Mar 13 14:09:01.648 CST: tty2 AAA/AUTHOR/CMD (2192867088): Method=LOCAL
Mar 13 14:09:01.648 CST: AAA/AUTHOR (2192867088): Post authorization status =
PASS_ADD
```

2.5 Implementing Local Router Accounting

These processes help you to accomplish the following tasks:

1. Configure basic local accounting for router access.
2. Verify and troubleshoot local accounting from VTY (Telnet) based access to the router.

Step 1 Configure basic local accounting for router access.

Include the following Cisco IOS configuration commands in your configuration to construct local based router accounting for EXEC and command authorization for privilege level 15 commands:

```
username rtr_super privilege level 15 password ciscorules

aaa new-model
aaa authentication login default local enable
aaa authentication login NO_AUTHENT none
aaa authorization exec default local if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 default local if-authenticated
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default start-stop group tacacs+
aaa accounting exec NO_ACCOUNT none
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting commands 15 NO_ACCOUNT none

line con 0
authorization commands 15 NO_AUTHOR
authorization exec NO_AUTHOR
accounting commands 1 NO_ACCOUNT
accounting commands 15 NO_ACCOUNT
accounting exec NO_ACCOUNT
login authentication NO_AUTHENT
```



Note In the preceding configuration fragment, the **start-stop** option is entered for EXEC shell sessions and the **stop-only** option is entered for privilege-level 15 commands. The router sends a start packet in the beginning of a shell service and a stop packet when the session terminates. A stop packet is only sent upon completion of a privilege level 15 command in the router. Additionally, note the use of the **NO_ACCOUNT** list to disable AAA accounting on the console port.

Step 2 Verify and troubleshoot local accounting from VTY (Telnet) based access to the router.

Enter the **debug aaa accounting** command to verify local router accounting is operating as expected. The following EXEC sequence illustrates that the appropriate commands are enabled:

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

The following tests illustrate operations described in “2.5 Implementing Local Router Accounting” and include relevant router output.

1. User rtr_super is authorized EXEC shell access.
2. User rtr_super successfully performs configure terminal, a privilege level 15 command.

The following diagnostic results are presented in the order in which they are generated during a typical authorization and command request process. Specific output fragments are separated out with brief explanatory notes to help you identify relevant information.



Note The **debug** command output can vary depending on Cisco IOS versions.

1. User *rtr_super* is authorized EXEC shell access.

Router **debug** output:

```
Apr 11 16:48:32.483: AAA/ACCT/EXEC/START User rtr_super, port tty3
Apr 11 16:48:32.483: AAA/ACCT/EXEC: Found list "default"
Apr 11 16:48:32.483: AAA/ACCT/EXEC/START User rtr_super, Port tty3, task_id=362
start_time=955471712 timezone=CST service=shell
Apr 11 16:48:32.483: AAA/ACCT: user rtr_super, acct type 0 (1526108857):
Method=tacacs+ (tacacs+)
Apr 11 16:48:33.487: TAC+: (1526108857): received acct response status = SUCCESS
```

2. User *rtr_super* successfully performs **configure terminal**, a privilege level 15 command.

Router **debug** output:

```
Apr 11 16:51:52.741: AAA/ACCT/CMD: User rtr_super, Port tty3, Priv 15: "configure
terminal <cr>"
Apr 11 16:51:52.741: AAA/ACCT/CMD: Found list "default"
Apr 11 16:51:52.741: AAA/ACCT: user rtr_super, acct type 3 (2701117300):
Method=tacacs+ (tacacs+)
Apr 11 16:51:53.545: TAC+: (2701117300): received acct response status = SUCCESS
```
