



Server-Based AAA Verification Diagnostic Output

This appendix is organized into the following sections:

- C.1 Server-Based TACACS+ Dialup Authentication Diagnostics
- C.2 Server-Based TACACS+ Dialup Authorization Diagnostics
- C.3 Server-Based RADIUS Dialup Authentication Diagnostics
- C.4 Server-Based RADIUS Dialup Authorization Diagnostics
- C.5 Server-Based TACACS+ Router Authentication Diagnostics
- C.6 Server-Based TACACS+ Router Authorization Diagnostics

Diagnostic examples present captured output from **debug** command (router) and **tail** command (AAA server) listings.



Note

Output fragments provided here are excerpted from the applicable **debug** command output or AAA server *csuslog* file—unless otherwise noted. Diagnostic content is gathered from the AAA server by using the **tail -f /var/log/csuslog** command. Pertinent portions of output are included as fragments of complete listings.

C.1 Server-Based TACACS+ Dialup Authentication Diagnostics

The following test results for “4.1 Implementing Server-Based TACACS+ Dialup Authentication” provide relevant NAS and AAA server log output:

1. Authentication login is successful for user tac_dial.
2. PAP authentication request for user tac_dial.
3. Creation of user tac_dial, service=ppp.
4. Authentication PASS received from AAA server.



Note

Use these **debug** commands: **debug aaa authentication** and **debug ppp authentication**.

The following diagnostic results are presented in the order in which they are generated during the authentication 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. Authentication login is successful for user *tac_dial*.

AAA server *csuslog* output:

```
Feb  4 10:40:13 coachella CiscoSecure: DEBUG - AUTHENTICATION START request
(8d2d325f)
Feb  4 10:40:13 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful;
[NAS = 172.22.63.1, Port = Async3, User = tac_dial, Priv = 1]
```

2. PAP authentication request for user *tac_dial*.

NAS **debug** output:

```
113288: Feb  4 10:40:13.696 CST: As3 PAP: I AUTH-REQ id 1 len 23 from "tac_dial"
113289: Feb  4 10:40:13.696 CST: As3 PAP: Authenticating peer tac_dial
```

3. Creation of user *tac_dial*, service=ppp.

NAS **debug** output:

```
113290: Feb  4 10:40:13.696 CST: AAA: parse name=Async3 idb type=10 tty=3
113291: Feb  4 10:40:13.696 CST: AAA: name=Async3 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=3 channel=0
113292: Feb  4 10:40:13.696 CST: AAA: parse name=Serial0:4 idb type=12 tty=-1
113293: Feb  4 10:40:13.696 CST: AAA: name=Serial0:4 flags=0x51 type=1 shelf=0 slot=0
adapter=0 port=0 channel=4
113294: Feb  4 10:40:13.696 CST: AAA/MEMORY: create_user (0x61E09254) user='tac_dial'
ruser='' port='Async3' rem_addr='async/81560' authen_type=PAP service=PPP priv=1
113295: Feb  4 10:40:13.696 CST: AAA/AUTHEN/START (2368549471): port='Async3' list=''
action=LOGIN service=PPP
```

4. Authentication PASS received from AAA server.

NAS **debug** output:

```
113296: Feb  4 10:40:13.696 CST: AAA/AUTHEN/START (2368549471): using "default" list
113297: Feb  4 10:40:13.696 CST: AAA/AUTHEN (2368549471): status = UNKNOWN
113298: Feb  4 10:40:13.696 CST: AAA/AUTHEN/START (2368549471): Method=tacacs+
(tacacs+)
113299: Feb  4 10:40:13.696 CST: TAC+: send AUTHEN/START packet ver=193 id=2368549471
113300: Feb  4 10:40:13.900 CST: TAC+: ver=193 id=2368549471 received AUTHEN status =
PASS
```

C.2 Server-Based TACACS+ Dialup Authorization Diagnostics

The following test results for “4.2 Implementing Server-Based TACACS+ Dialup Authorization” provide relevant NAS and AAA server log output:

1. User dialtest is authorized EXEC shell access to the NAS.
2. User dialtest starts PPP from the shell and is assigned the addr-pool=default and inacl=110 AVPs.
3. User dialtest is authorized EXEC shell access to NAS.
4. User dialtest is assigned the addr-pool=default AVP through network authorization.

5. User *dialtest* is assigned the `inac1=110` AVP through network authorization.
6. User *dialtest* starts PPP and is assigned the `addr-pool=default` and `inac1=110` AVPs.



Note Use this **debug** command: **debug aaa authorization**.

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 *dialtest* is authorized EXEC shell access to the NAS.

AAA server *csuslog* output:

```
Apr 6 15:48:06 sleddog CiscoSecure: DEBUG - AUTHORIZATION request (365f23d3)
Apr 6 15:48:06 sleddog CiscoSecure: DEBUG - Authorization - Request authorized; [NAS
= 172.23.84.35, user = dialtest, port = tty8, input: service=shell cmd* output: ]
```

2. User *dialtest* starts PPP from the shell and is assigned the `addr-pool=default` and `inac1=110` AVPs.

AAA server *csuslog* output:

```
Apr 6 15:48:07 sleddog CiscoSecure: DEBUG - AUTHORIZATION request (74e5f744)
Apr 6 15:48:07 sleddog CiscoSecure: DEBUG - Authorization - Request authorized; [NAS
= 172.23.84.35, user = dialtest, port = tty8, input: service=ppp protocol=ip
addr-pool*default output: inac1=110]
Apr 6 15:48:13 sleddog CiscoSecure: DEBUG - AUTHORIZATION request (78655fcd)
Apr 6 15:48:13 sleddog CiscoSecure: DEBUG - Authorization - Request authorized; [NAS
= 172.23.84.35, user = dialtest, port = tty8, input: service=ppp protocol=lcp output:
]
Apr 6 15:48:13 sleddog CiscoSecure: DEBUG - AUTHORIZATION request (cae30c69)
Apr 6 15:48:13 sleddog CiscoSecure: DEBUG - Authorization - Request authorized; [NAS
= 172.23.84.35, user = dialtest, port = tty8, input: service=ppp protocol=ip output:
addr-pool=default inac1=110]
```

3. User *dialtest* is authorized EXEC shell access to NAS.

NAS **debug** output:

```
*Apr 6 00:12:29.932: As8 AAA/AUTHOR/EXEC (912204755): Port='tty8' list=''
service=EXEC
*Apr 6 00:12:29.932: AAA/AUTHOR/EXEC: As8 (912204755) user='dialtest'
*Apr 6 00:12:29.932: As8 AAA/AUTHOR/EXEC (912204755): send AV service=shell
*Apr 6 00:12:29.932: As8 AAA/AUTHOR/EXEC (912204755): send AV cmd*
*Apr 6 00:12:29.932: As8 AAA/AUTHOR/EXEC (912204755): found list "default"
*Apr 6 00:12:29.932: As8 AAA/AUTHOR/EXEC (912204755): Method=tacacs+ (tacacs+)
*Apr 6 00:12:29.932: AAA/AUTHOR/TAC+: (912204755): user=dialtest
*Apr 6 00:12:29.932: AAA/AUTHOR/TAC+: (912204755): send AV service=shell
*Apr 6 00:12:29.932: AAA/AUTHOR/TAC+: (912204755): send AV cmd*
*Apr 6 00:12:30.136: As8 AAA/AUTHOR (912204755): Post authorization status =
PASS_ADD
```

- User *dialtest* is assigned the **addr-pool=default** AVP through network authorization.

NAS debug output:

```
*Apr 6 00:12:31.480: AAA/AUTHOR/PPP: As8 (1961228100) user='dialtest'
*Apr 6 00:12:31.480: As8 AAA/AUTHOR/PPP (1961228100): send AV service=ppp
*Apr 6 00:12:31.480: As8 AAA/AUTHOR/PPP (1961228100): send AV protocol=ip
*Apr 6 00:12:31.480: As8 AAA/AUTHOR/PPP (1961228100): send AV addr-pool*default
*Apr 6 00:12:31.480: As8 AAA/AUTHOR/PPP (1961228100): found list "default"
*Apr 6 00:12:31.480: As8 AAA/AUTHOR/PPP (1961228100): Method=tacacs+ (tacacs+)
*Apr 6 00:12:31.480: AAA/AUTHOR/TAC+: (1961228100): user=dialtest
*Apr 6 00:12:31.480: AAA/AUTHOR/TAC+: (1961228100): send AV service=ppp
*Apr 6 00:12:31.480: AAA/AUTHOR/TAC+: (1961228100): send AV protocol=ip
*Apr 6 00:12:31.480: AAA/AUTHOR/TAC+: (1961228100): send AV addr-pool*default
*Apr 6 00:12:31.684: As8 AAA/AUTHOR (1961228100): Post authorization status =
PASS_ADD
```

- User *dialtest* is assigned the **inac1=110** AVP through network authorization.

NAS debug output:

```
*Apr 6 00:12:31.684: AAA/AUTHOR/Async8: PPP: Processing AV service=ppp
*Apr 6 00:12:31.684: AAA/AUTHOR/Async8: PPP: Processing AV protocol=ip
*Apr 6 00:12:31.684: AAA/AUTHOR/Async8: PPP: Processing AV addr-pool*default
*Apr 6 00:12:31.684: AAA/AUTHOR/Async8: PPP: Processing AV inac1=110
```

- User *dialtest* starts PPP and is assigned the **addr-pool=default** and **inac1=110** AVPs.

NAS debug output:

```
*Apr 6 00:33:05.860: As9 AAA/AUTHOR/IPCP: Says use pool default
*Apr 6 00:33:05.864: As9 AAA/AUTHOR/IPCP: Pool returned 172.23.25.37
*Apr 6 00:33:05.864: As9 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Apr 6 00:33:05.864: As9 AAA/AUTHOR/IPCP: Processing AV protocol=ip
*Apr 6 00:33:05.864: As9 AAA/AUTHOR/IPCP: Processing AV addr-pool=default
*Apr 6 00:33:05.864: As9 AAA/AUTHOR/IPCP: Processing AV inac1=110
*Apr 6 00:33:05.864: As9 AAA/AUTHOR/IPCP: Processing AV addr*172.23.25.37
*Apr 6 00:33:05.864: As9 AAA/AUTHOR/IPCP: Authorization succeeded
```

C.3 Server-Based RADIUS Dialup Authentication Diagnostics

The following test results for “4.3 Implementing Server-Based RADIUS Dialup Authentication” provide relevant NAS output:

- User *rad_dial* successfully passes authentication on port Async 5).
- User *rad_dial* successfully passes authentication.



Note Use these **debug** commands: **debug aaa authentication** and **debug ppp authentication**.

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



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

1. User *rad_dial* successfully passes authentication on port Async 5).

NAS **debug** output:

```
00:38:42: AAA/MEMORY: create_user (0x61619F48) user='rad_dial' ruser='' port='Async5'
rem_addr='65004/65301' authen_type=PAP service=PPP priv=1
00:38:42: AAA/AUTHEN/START (3896270890): port='Async5' list='' action=LOGIN
service=PPP
00:38:42: AAA/AUTHEN/START (3896270890): using "default" list
00:38:42: AAA/AUTHEN (3896270890): status = UNKNOWN
00:38:42: AAA/AUTHEN/START (3896270890): Method=radius (radius)
00:38:42: AAA/AUTHEN (3896270890): status = PASS
```

2. User *rad_dial* successfully passes authentication.

NAS **debug** output:

```
Apr 6 16:18:19 danvers CiscoSecure: INFO - Profile: user = rad_dial {
Apr 6 16:18:19 danvers          set server current-failed-logins = 0
Apr 6 16:18:19 danvers profile_cycle = 9
```

C.4 Server-Based RADIUS Dialup Authorization Diagnostics

The following test results for “4.4 Implementing Server-Based RADIUS Dialup Authorization” provide relevant NAS server log output:

1. User *rad_dial* is authorized for protocol=lcp.
2. User *rad_dial* is authorized for IPCP.
3. Input access-list is verified as 110 while the output access-list is shown as not set.



Note Use these commands: **debug aaa authorization** and **show caller user rad_dial detail**.

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 you identify relevant information.



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

1. User *rad_dial* is authorized for **protocol=lcp**.

NAS debug output:

```
01:02:17: AAA/MEMORY: create_user (0x61504AC4) user='rad_dial' ruser='' port='Async6' rem_addr='65004/65301' authn_type=PAP service=PPP priv=1
01:02:17: As6 AAA/AUTHOR/LCP: Authorize LCP
01:02:17: As6 AAA/AUTHOR/LCP (3341570658): Port='Async6' list='' service=NET
01:02:17: AAA/AUTHOR/LCP: As6 (3341570658) user='rad_dial'
01:02:17: As6 AAA/AUTHOR/LCP (3341570658): send AV service=ppp
01:02:17: As6 AAA/AUTHOR/LCP (3341570658): send AV protocol=lcp
01:02:17: As6 AAA/AUTHOR/LCP (3341570658): found list "default"
01:02:17: As6 AAA/AUTHOR/LCP (3341570658): Method=radius (radius)
01:02:17: As6 AAA/AUTHOR (3341570658): Post authorization status = PASS_REPL
```

2. User *rad_dial* is authorized for IPCP.

NAS debug output:

```
01:02:17: As6 AAA/AUTHOR/LCP: Processing AV service=ppp
01:02:17: As6 AAA/AUTHOR/FSM: (0): Can we start IPCP?
01:02:17: As6 AAA/AUTHOR/FSM (2347737596): Port='Async6' list='' service=NET
01:02:17: AAA/AUTHOR/FSM: As6 (2347737596) user='rad_dial'
01:02:17: As6 AAA/AUTHOR/FSM (2347737596): send AV service=ppp
01:02:17: As6 AAA/AUTHOR/FSM (2347737596): send AV protocol=ip
01:02:17: As6 AAA/AUTHOR/FSM (2347737596): found list "default"
01:02:17: As6 AAA/AUTHOR/FSM (2347737596): Method=radius (radius)
01:02:17: As6 AAA/AUTHOR (2347737596): Post authorization status = PASS_REPL
01:02:17: As6 AAA/AUTHOR/FSM: We can start IPCP
01:02:17: As6 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 172.22.83.5
01:02:17: As6 AAA/AUTHOR/IPCP: Processing AV service=ppp
01:02:17: As6 AAA/AUTHOR/IPCP: Processing AV inacl=110
01:02:17: As6 AAA/AUTHOR/IPCP: Authorization succeeded
01:02:17: As6 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 172.22.83.5
01:02:18: As6 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 172.22.83.5
01:02:18: As6 AAA/AUTHOR/IPCP: Processing AV service=ppp
01:02:18: As6 AAA/AUTHOR/IPCP: Processing AV inacl=110
01:02:18: As6 AAA/AUTHOR/IPCP: Authorization succeeded
01:02:18: As6 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 172.22.83.5
01:02:18: As6 AAA/AUTHOR/IPCP: Start. Her address 172.22.83.5, we want 172.22.8 3.5
```

3. Input access-list is verified as 110 while the output access-list is shown as not set.

Output from `show caller user rad_dial detail` from NAS:

```

User: rad_dial, line tty 116, service Async
  Active time 00:01:29, Idle time 00:00:40
Timeouts:          Absolute  Idle      Idle
                   Session   Exec
Limits:           04:00:00  -        00:48:00
Disconnect in:    03:58:30  -        -
TTY: Line 116, running PPP on As116
Location: PPP: 172.22.83.37
DS0: (slot/unit/channel)=0/0/20
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 As116, service PPP
  Active time 00:01:23, Idle time 00:00:35
Timeouts:          Absolute  Idle
Limits:           -        -
Disconnect in:    -        -
PPP: LCP Open, PAP (<- AAA), IPCP, CDPCP
LCP: -> peer, ACCM, AuthProto, MagicNumber, PCompression, ACCompression
     <- peer, ACCM, MagicNumber, PCompression, ACCompression
NCP: Open IPCP, CDPCP
IPCP: <- peer, Address
     -> peer, Address
IP: Local 172.22.83.1, remote 172.22.83.37
   Access list (I/O) is 110/not set, default (I/O) not set/not set
Counts: 14 packets input, 1399 bytes, 0 no buffer
        1 input errors, 1 CRC, 0 frame, 0 overrun
        15 packets output, 1448 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets

```

C.5 Server-Based TACACS+ Router Authentication Diagnostics

The following test results for “4.5 Implementing Server-Based TACACS+ Router Authentication” provide relevant router output:

1. Get user and password interaction between router and AAA server.
2. User `rtr_test` successfully logs in.



Note Use this **debug** command: **debug aaa authentication**.

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



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

1. Get user and password interaction between router and AAA server.

Router debug output:

```

Feb 24 11:10:27.101 CST: AAA/MEMORY: create_user (0x61F74900) user='' ruser=''
port='tty2' rem_addr='172.22.53.201' authen_type=ASCII service=LOGIN priv=1
Feb 24 11:10:27.101 CST: AAA/AUTHEN/START (2925282821): port='tty2' list=''
action=LOGIN service=LOGIN
Feb 24 11:10:27.101 CST: AAA/AUTHEN/START (2925282821): using "default" list
Feb 24 11:10:27.101 CST: AAA/AUTHEN/START (2925282821): Method=tacacs+ (tacacs+)
Feb 24 11:10:27.105 CST: TAC+: send AUTHEN/START packet ver=192 id=2925282821
Feb 24 11:10:27.305 CST: TAC+: ver=192 id=2925282821 received AUTHEN status = GETUSER
Feb 24 11:10:27.305 CST: AAA/AUTHEN (2925282821): status = GETUSER
Feb 24 11:10:30.549 CST: AAA/AUTHEN/CONT (2925282821): continue_login
(user='(undef)')
Feb 24 11:10:30.549 CST: AAA/AUTHEN (2925282821): status = GETUSER
Feb 24 11:10:30.549 CST: AAA/AUTHEN (2925282821): Method=tacacs+ (tacacs+)
Feb 24 11:10:30.549 CST: TAC+: send AUTHEN/CONT packet id=2925282821
Feb 24 11:10:30.749 CST: TAC+: ver=192 id=2925282821 received AUTHEN status = GETPASS
Feb 24 11:10:30.749 CST: AAA/AUTHEN (2925282821): status = GETPASS
Feb 24 11:10:33.981 CST: AAA/AUTHEN/CONT (2925282821): continue_login
(user='rtr_test')
Feb 24 11:10:33.981 CST: AAA/AUTHEN (2925282821): status = GETPASS
Feb 24 11:10:33.981 CST: AAA/AUTHEN (2925282821): Method=tacacs+ (tacacs+)
Feb 24 11:10:33.981 CST: TAC+: send AUTHEN/CONT packet id=2925282821
Feb 24 11:10:34.181 CST: TAC+: ver=192 id=2925282821 received AUTHEN status = PASS
Feb 24 11:10:34.181 CST: AAA/AUTHEN (2925282821): status = PASS
Feb 24 11:10:34.381 CST: TAC+: (2248458861): received author response status =
PASS_ADD

```

2. User *rtr_test* successfully logs in.AAA server *csuslog* output:

```

Feb 24 11:10:34 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful;
[NAS = 172.22.255.3, Port = tty2, User = rtr_test, Priv = 1

```

C.6 Server-Based TACACS+ Router Authorization Diagnostics

The following test results illustrate three separate user types as described in “4.6 Implementing Server-Based TACACS+ Router Authorization”, belonging to three separate user groups: *rtr_low*, *rtr_tech*, and *rtr_super*. The example output is provided in the following sections:

- C.6.1 Test Results for *rtr_low* Group
- C.6.2 Test Results for *rtr_tech* Group
- C.6.3 Test Results for *rtr_super* Group



Note Use this **debug** command: **debug aaa authorization**.

C.6.1 Test Results for *rtr_low* Group

Test results follow for each Cisco IOS command summarized in Table 4-1, including relevant router output and AAA server log output:

1. User *rtr_dweeb* is authorized EXEC shell access.
2. User *rtr_dweeb* enters enable mode.
3. User *rtr_dweeb* fails debug all command.
4. User *rtr_dweeb* fails debug ip packet command.
5. User *rtr_dweeb* fails clear ip cache command.
6. User *rtr_dweeb* fails reload command.
7. User *rtr_dweeb* fails show running-config command.
8. User *rtr_dweeb* fails write terminal command.
9. User *rtr_dweeb* fails copy running-config startup-config command.
10. User *rtr_dweeb* fails write memory command.
11. User *rtr_dweeb* fails configure terminal 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_dweeb* is authorized EXEC shell access.

Router **debug** output:

```
Feb 18 11:44:36.115 CST: AAA/MEMORY: create_user (0x61F883B4) user='' ruser='' port='tty3' rem_addr='172.22.53.201' authn_type=ASCII service=LOGIN priv=1
Feb 18 11:44:42.135 CST: tty3 AAA/AUTHOR/EXEC (1279405337): Port='tty3' list='service=EXEC
Feb 18 11:44:42.135 CST: AAA/AUTHOR/EXEC: tty3 (1279405337) user='rtr_dweeb'
Feb 18 11:44:42.135 CST: tty3 AAA/AUTHOR/EXEC (1279405337): send AV service=shell
Feb 18 11:44:42.135 CST: tty3 AAA/AUTHOR/EXEC (1279405337): send AV cmd*
Feb 18 11:44:42.135 CST: tty3 AAA/AUTHOR/EXEC (1279405337): found list "default"
Feb 18 11:44:42.135 CST: tty3 AAA/AUTHOR/EXEC (1279405337): Method=tacacs+ (tacacs+)
Feb 18 11:44:42.135 CST: AAA/AUTHOR/TAC+: (1279405337): user=rtr_dweeb
Feb 18 11:44:42.135 CST: AAA/AUTHOR/TAC+: (1279405337): send AV service=shell
Feb 18 11:44:42.135 CST: AAA/AUTHOR/TAC+: (1279405337): send AV cmd*
Feb 18 11:44:42.335 CST: AAA/AUTHOR (1279405337): Post authorization status = PASS_ADD
Feb 18 11:44:42.335 CST: AAA/AUTHOR/EXEC: Authorization successful
```

AAA server *csuslog* output:

```
Feb 18 11:44:41 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful; [NAS = 172.22.255.3, Port = tty3, User = rtr_dweeb, Priv = 1]
Feb 18 11:44:41 coachella CiscoSecure: DEBUG -
Feb 18 11:44:42 coachella CiscoSecure: DEBUG - AUTHORIZATION request (4c422d19)
Feb 18 11:44:42 coachella CiscoSecure: DEBUG - Authorization - Request authorized; [NAS = 172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell cmd* output: ]
```

2. User *rtr_dweeb* enters **enable** mode.

Router **debug** output:

```
Feb 18 11:44:45.651 CST: AAA/MEMORY: free_user (0x61CC44D4) user='' ruser='' port='tty3' rem_addr='172.22.53.201' authn_type=ASCII service=ENABLE priv=15
```

3. User *rtr_dweeb* fails **debug all** command.

Router **debug** output:

```
Feb 18 11:44:49.875 CST: tty3 AAA/AUTHOR/CMD (2800178490): Port='tty3' list='' service=CMD
Feb 18 11:44:49.875 CST: AAA/AUTHOR/CMD: tty3 (2800178490) user='rtr_dweeb'
Feb 18 11:44:49.875 CST: tty3 AAA/AUTHOR/CMD (2800178490): send AV service=shell
Feb 18 11:44:49.879 CST: tty3 AAA/AUTHOR/CMD (2800178490): send AV cmd=debug
Feb 18 11:44:49.879 CST: tty3 AAA/AUTHOR/CMD (2800178490): send AV cmd-arg=all
Feb 18 11:44:49.879 CST: tty3 AAA/AUTHOR/CMD (2800178490): send AV cmd-arg=<cr>
Feb 18 11:44:49.879 CST: tty3 AAA/AUTHOR/CMD (2800178490): found list "default"
Feb 18 11:44:49.879 CST: tty3 AAA/AUTHOR/CMD (2800178490): Method=tacacs+ (tacacs+)
Feb 18 11:44:49.879 CST: AAA/AUTHOR/TAC+: (2800178490): user=rtr_dweeb
Feb 18 11:44:49.879 CST: AAA/AUTHOR/TAC+: (2800178490): send AV service=shell
Feb 18 11:44:49.879 CST: AAA/AUTHOR/TAC+: (2800178490): send AV cmd=debug
Feb 18 11:44:49.879 CST: AAA/AUTHOR/TAC+: (2800178490): send AV cmd-arg=all
Feb 18 11:44:49.879 CST: AAA/AUTHOR/TAC+: (2800178490): send AV cmd-arg=<cr>
Feb 18 11:44:50.079 CST: AAA/AUTHOR (2800178490): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:44:49 coachella CiscoSecure: DEBUG - AUTHORIZATION request (a6e7553a)
Feb 18 11:44:49 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell cmd=debug
cmd-arg=all cmd-arg=<cr> output: ]
```

4. User *rtr_dweeb* fails **debug ip packet** command.

Router **debug** output:

```
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): Port='tty3' list=''
service=CMD
Feb 18 11:44:55.447 CST: AAA/AUTHOR/CMD: tty3 (4087104408) user='rtr_dweeb'
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): send AV service=shell
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): send AV cmd=debug
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): send AV cmd-arg=ip
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): send AV cmd-arg=packet
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): send AV cmd-arg=<cr>
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): found list "default"
Feb 18 11:44:55.447 CST: tty3 AAA/AUTHOR/CMD (4087104408): Method=tacacs+ (tacacs+)
Feb 18 11:44:55.447 CST: AAA/AUTHOR/TAC+: (4087104408): user=rtr_dweeb
Feb 18 11:44:55.447 CST: AAA/AUTHOR/TAC+: (4087104408): send AV service=shell
Feb 18 11:44:55.447 CST: AAA/AUTHOR/TAC+: (4087104408): send AV cmd=debug
Feb 18 11:44:55.447 CST: AAA/AUTHOR/TAC+: (4087104408): send AV cmd-arg=ip
Feb 18 11:44:55.447 CST: AAA/AUTHOR/TAC+: (4087104408): send AV cmd-arg=packet
Feb 18 11:44:55.447 CST: AAA/AUTHOR/TAC+: (4087104408): send AV cmd-arg=<cr>
Feb 18 11:44:55.647 CST: AAA/AUTHOR (4087104408): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:44:55 coachella CiscoSecure: DEBUG - AUTHORIZATION request (f39c4398)
Feb 18 11:44:55 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell cmd=debug
cmd-arg=ip cmd-arg=packet cmd-arg=<cr> output: ]
```

5. User *rtr_dweeb* fails **clear ip cache** command.

Router **debug** output:

```
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): Port='tty3'
list='' service=CMD
Feb 18 11:45:00.483 CST: AAA/AUTHOR/CMD: tty3 (3223867754) user='rtr_dweeb'
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): send AV service=shell
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): send AV cmd=clear
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): send AV cmd-arg=ip
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): send AV cmd-arg=cache
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): send AV cmd-arg=<cr>
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): found list "default"
Feb 18 11:45:00.483 CST: tty3 AAA/AUTHOR/CMD (3223867754): Method=tacacs+ (tacacs+)
Feb 18 11:45:00.483 CST: AAA/AUTHOR/TAC+: (3223867754): user=rtr_dweeb
Feb 18 11:45:00.483 CST: AAA/AUTHOR/TAC+: (3223867754): send AV service=shell
Feb 18 11:45:00.483 CST: AAA/AUTHOR/TAC+: (3223867754): send AV cmd=clear
Feb 18 11:45:00.483 CST: AAA/AUTHOR/TAC+: (3223867754): send AV cmd-arg=ip
Feb 18 11:45:00.483 CST: AAA/AUTHOR/TAC+: (3223867754): send AV cmd-arg=cache
Feb 18 11:45:00.483 CST: AAA/AUTHOR/TAC+: (3223867754): send AV cmd-arg=<cr>
Feb 18 11:45:00.687 CST: AAA/AUTHOR (3223867754): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:45:00 coachella CiscoSecure: DEBUG - AUTHORIZATION request (c028516a)
Feb 18 11:45:00 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell cmd=clear
cmd-arg=ip cmd-arg=cache cmd-arg=<cr> output: ]
```

6. User *rtr_dweeb* fails **reload** command.Router **debug** output:

```
Feb 18 11:45:03.911 CST: tty3 AAA/AUTHOR/CMD (410330894): Port='tty3' list=''
service=CMD
Feb 18 11:45:03.911 CST: AAA/AUTHOR/CMD: tty3 (410330894) user='rtr_dweeb'
Feb 18 11:45:03.911 CST: tty3 AAA/AUTHOR/CMD (410330894): send AV service=shell
Feb 18 11:45:03.911 CST: tty3 AAA/AUTHOR/CMD (410330894): send AV cmd=reload
Feb 18 11:45:03.911 CST: tty3 AAA/AUTHOR/CMD (410330894): send AV cmd-arg=<cr>
Feb 18 11:45:03.911 CST: tty3 AAA/AUTHOR/CMD (410330894): found list "default"
Feb 18 11:45:03.911 CST: tty3 AAA/AUTHOR/CMD (410330894): Method=tacacs+ (tacacs+)
Feb 18 11:45:03.911 CST: AAA/AUTHOR/TAC+: (410330894): user=rtr_dweeb
Feb 18 11:45:03.911 CST: AAA/AUTHOR/TAC+: (410330894): send AV service=shell
Feb 18 11:45:03.911 CST: AAA/AUTHOR/TAC+: (410330894): send AV cmd=reload
Feb 18 11:45:03.911 CST: AAA/AUTHOR/TAC+: (410330894): send AV cmd-arg=<cr>
Feb 18 11:45:04.115 CST: AAA/AUTHOR (410330894): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:45:03 coachella CiscoSecure: DEBUG - AUTHORIZATION request (1875270e)
Feb 18 11:45:03 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell cmd=reload
cmd-arg=<cr> output: ]
```

7. User *rtr_dweeb* fails **show running-config** command.Router **debug** output:

```
Feb 18 11:45:08.891 CST: tty3 AAA/AUTHOR/CMD (2227741892): Port='tty3' list=''
service=CMD
Feb 18 11:45:08.891 CST: AAA/AUTHOR/CMD: tty3 (2227741892) user='rtr_dweeb'
Feb 18 11:45:08.891 CST: tty3 AAA/AUTHOR/CMD (2227741892): send AV service=shell
Feb 18 11:45:08.891 CST: tty3 AAA/AUTHOR/CMD (2227741892): send AV cmd=show
Feb 18 11:45:08.891 CST: tty3 AAA/AUTHOR/CMD (2227741892): send AV
cmd-arg=running-config
Feb 18 11:45:08.891 CST: tty3 AAA/AUTHOR/CMD (2227741892): send AV cmd-arg=<cr>
Feb 18 11:45:08.891 CST: tty3 AAA/AUTHOR/CMD (2227741892): found list "default"
Feb 18 11:45:08.891 CST: tty3 AAA/AUTHOR/CMD (2227741892): Method=tacacs+ (tacacs+)
Feb 18 11:45:08.891 CST: AAA/AUTHOR/TAC+: (2227741892): user=rtr_dweeb
Feb 18 11:45:08.891 CST: AAA/AUTHOR/TAC+: (2227741892): send AV service=shell
Feb 18 11:45:08.891 CST: AAA/AUTHOR/TAC+: (2227741892): send AV cmd=show
Feb 18 11:45:08.891 CST: AAA/AUTHOR/TAC+: (2227741892): send AV
cmd-arg=running-config
Feb 18 11:45:08.891 CST: AAA/AUTHOR/TAC+: (2227741892): send AV cmd-arg=<cr>
Feb 18 11:45:09.095 CST: AAA/AUTHOR (2227741892): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:45:08 coachella CiscoSecure: DEBUG - AUTHORIZATION request (84c8a4c4)
Feb 18 11:45:08 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell
cmd=showcmd-arg=running-config cmd-arg=<cr> output: ]
```

8. User *rtr_dweeb* fails **write terminal** command.Router **debug** output:

```
Feb 18 11:45:12.079 CST: tty3 AAA/AUTHOR/CMD (2744233862): Port='tty3' list=''
service=CMD
Feb 18 11:45:12.079 CST: AAA/AUTHOR/CMD: tty3 (2744233862) user='rtr_dweeb'
Feb 18 11:45:12.079 CST: tty3 AAA/AUTHOR/CMD (2744233862): send AV service=shell
Feb 18 11:45:12.079 CST: tty3 AAA/AUTHOR/CMD (2744233862): send AV cmd=write
Feb 18 11:45:12.079 CST: tty3 AAA/AUTHOR/CMD (2744233862): send AV cmd-arg=terminal
Feb 18 11:45:12.079 CST: tty3 AAA/AUTHOR/CMD (2744233862): send AV cmd-arg=<cr>
Feb 18 11:45:12.079 CST: tty3 AAA/AUTHOR/CMD (2744233862): found list "default"
Feb 18 11:45:12.079 CST: tty3 AAA/AUTHOR/CMD (2744233862): Method=tacacs+ (tacacs+)
Feb 18 11:45:12.079 CST: AAA/AUTHOR/TAC+: (2744233862): user=rtr_dweeb
Feb 18 11:45:12.079 CST: AAA/AUTHOR/TAC+: (2744233862): send AV service=shell
Feb 18 11:45:12.079 CST: AAA/AUTHOR/TAC+: (2744233862): send AV cmd=write
Feb 18 11:45:12.079 CST: AAA/AUTHOR/TAC+: (2744233862): send AV cmd-arg=terminal
Feb 18 11:45:12.079 CST: AAA/AUTHOR/TAC+: (2744233862): send AV cmd-arg=<cr>
Feb 18 11:45:12.279 CST: AAA/AUTHOR (2744233862): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:45:11 coachella CiscoSecure: DEBUG - AUTHORIZATION request (a391af86)
Feb 18 11:45:11 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell cmd=write
cmd-arg=terminal cmd-arg=<cr> output: ]
```

9. User *rtr_dweeb* fails **copy running-config startup-config** command.Router **debug** output:

```
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): Port='tty3' list=''
service=CMD
Feb 18 11:45:17.631 CST: AAA/AUTHOR/CMD: tty3 (1138992853) user='rtr_dweeb'
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): send AV service=shell
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): send AV cmd=copy
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): send AV
cmd-arg=running-config
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): send AV
cmd-arg=startup-config
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): send AV cmd-arg=<cr>
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): found list "default"
Feb 18 11:45:17.631 CST: tty3 AAA/AUTHOR/CMD (1138992853): Method=tacacs+ (tacacs+)
Feb 18 11:45:17.631 CST: AAA/AUTHOR/TAC+: (1138992853): user=rtr_dweeb
Feb 18 11:45:17.631 CST: AAA/AUTHOR/TAC+: (1138992853): send AV service=shell
Feb 18 11:45:17.631 CST: AAA/AUTHOR/TAC+: (1138992853): send AV cmd=copy
Feb 18 11:45:17.631 CST: AAA/AUTHOR/TAC+: (1138992853): send AV
cmd-arg=running-config
Feb 18 11:45:17.631 CST: AAA/AUTHOR/TAC+: (1138992853): send AV
cmd-arg=startup-config
Feb 18 11:45:17.631 CST: AAA/AUTHOR/TAC+: (1138992853): send AV cmd-arg=<cr>
Feb 18 11:45:17.835 CST: AAA/AUTHOR (1138992853): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:45:17 coachella CiscoSecure: DEBUG - AUTHORIZATION request (43e3a6d5)
Feb 18 11:45:17 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell
cmd=copycmd-arg=running-config cmd-arg=startup-config cmd-arg=<cr> output: ]
```

10. User *rtr_dweeb* fails **write memory** command.Router **debug** output:

```
Feb 18 11:45:20.915 CST: tty3 AAA/AUTHOR/CMD (1068431717): Port='tty3' list=''
service=CMD
Feb 18 11:45:20.915 CST: AAA/AUTHOR/CMD: tty3 (1068431717) user='rtr_dweeb'
Feb 18 11:45:20.915 CST: tty3 AAA/AUTHOR/CMD (1068431717): send AV service=shell
Feb 18 11:45:20.915 CST: tty3 AAA/AUTHOR/CMD (1068431717): send AV cmd=write
Feb 18 11:45:20.915 CST: tty3 AAA/AUTHOR/CMD (1068431717): send AV cmd-arg=memory
Feb 18 11:45:20.915 CST: tty3 AAA/AUTHOR/CMD (1068431717): send AV cmd-arg=<cr>
Feb 18 11:45:20.915 CST: tty3 AAA/AUTHOR/CMD (1068431717): found list "default"
Feb 18 11:45:20.915 CST: tty3 AAA/AUTHOR/CMD (1068431717): Method=tacacs+ (tacacs+)
Feb 18 11:45:20.915 CST: AAA/AUTHOR/TAC+: (1068431717): user=rtr_dweeb
Feb 18 11:45:20.915 CST: AAA/AUTHOR/TAC+: (1068431717): send AV service=shell
Feb 18 11:45:20.915 CST: AAA/AUTHOR/TAC+: (1068431717): send AV cmd=write
Feb 18 11:45:20.915 CST: AAA/AUTHOR/TAC+: (1068431717): send AV cmd-arg=memory
Feb 18 11:45:20.915 CST: AAA/AUTHOR/TAC+: (1068431717): send AV cmd-arg=<cr>
Feb 18 11:45:21.119 CST: AAA/AUTHOR (1068431717): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:45:20 coachella CiscoSecure: DEBUG - AUTHORIZATION request (3faef965)
Feb 18 11:45:20 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell
cmd=writecmd-arg=memory cmd-arg=<cr> output: ]
```

11. User *rtr_dweeb* fails **configure terminal** command.Router **debug** output:

```
Feb 18 11:45:32.399 CST: tty3 AAA/AUTHOR/CMD (530570549): Port='tty3' list=''
service=CMD
Feb 18 11:45:32.399 CST: AAA/AUTHOR/CMD: tty3 (530570549) user='rtr_dweeb'
Feb 18 11:45:32.399 CST: tty3 AAA/AUTHOR/CMD (530570549): send AV service=shell
Feb 18 11:45:32.399 CST: tty3 AAA/AUTHOR/CMD (530570549): send AV cmd=configure
Feb 18 11:45:32.399 CST: tty3 AAA/AUTHOR/CMD (530570549): send AV cmd-arg=terminal
Feb 18 11:45:32.399 CST: tty3 AAA/AUTHOR/CMD (530570549): send AV cmd-arg=<cr>
Feb 18 11:45:32.399 CST: tty3 AAA/AUTHOR/CMD (530570549): found list "default"
Feb 18 11:45:32.399 CST: tty3 AAA/AUTHOR/CMD (530570549): Method=tacacs+ (tacacs+)
Feb 18 11:45:32.399 CST: AAA/AUTHOR/TAC+: (530570549): user=rtr_dweeb
Feb 18 11:45:32.399 CST: AAA/AUTHOR/TAC+: (530570549): send AV service=shell
Feb 18 11:45:32.399 CST: AAA/AUTHOR/TAC+: (530570549): send AV cmd=configure
Feb 18 11:45:32.399 CST: AAA/AUTHOR/TAC+: (530570549): send AV cmd-arg=terminal
Feb 18 11:45:32.399 CST: AAA/AUTHOR/TAC+: (530570549): send AV cmd-arg=<cr>
Feb 18 11:45:32.603 CST: AAA/AUTHOR (530570549): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 11:45:32 coachella CiscoSecure: DEBUG - AUTHORIZATION request (1f9fdd35)
Feb 18 11:45:32 coachella CiscoSecure: DEBUG - Authorization - Failed command; [NAS =
172.22.255.3, user = rtr_dweeb, port = tty3, input: service=shell cmd=configure
cmd-arg=terminal cmd-arg=<cr> output: ]
```

C.6.2 Test Results for *rtr_tech* Group

Tests results follow for each of the Cisco IOS commands summarized in Table 4-1, including relevant router output and AAA server log output:

1. User *rtr_techie* is authorized EXEC shell access.
2. User *rtr_techie* enters enable mode.
3. User *rtr_techie* is denied the debug all command.

4. User `rtr_techie` is permitted `debug ip packet` command.
5. User `rtr_techie` is permitted `clear ip cache` command.
6. User `rtr_techie` is denied `reload` command.
7. User `rtr_techie` is permitted `show running-config` command.
8. User `rtr_techie` is permitted `write terminal` command.
9. User `rtr_techie` is permitted `copy running-config starting config` command.
10. User `rtr_techie` is permitted `write memory` command.
11. User `rtr_techie` is denied `configure terminal` 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_techie` is authorized EXEC shell access.

Router **debug** output:

```
Feb 18 14:27:32.388 CST: AAA/MEMORY: create_user (0x61CC44D8) user='' ruser=''
port='tty3' rem_addr='172.22.53.201' authen_type=ASCII service=LOGIN priv=1
Feb 18 14:27:36.984 CST: tty3 AAA/AUTHOR/EXEC (3820424789): Port='tty3'
list=''service=EXEC
Feb 18 14:27:36.984 CST: AAA/AUTHOR/EXEC: tty3 (3820424789) user='rtr_techie'
Feb 18 14:27:36.984 CST: tty3 AAA/AUTHOR/EXEC (3820424789): send AV service=shell
Feb 18 14:27:36.984 CST: tty3 AAA/AUTHOR/EXEC (3820424789): send AV cmd*
Feb 18 14:27:36.984 CST: tty3 AAA/AUTHOR/EXEC (3820424789): found list "default"
Feb 18 14:27:36.984 CST: tty3 AAA/AUTHOR/EXEC (3820424789): Method=tacacs+ (tacacs+)
Feb 18 14:27:36.984 CST: AAA/AUTHOR/TAC+: (3820424789): user=rtr_techie
Feb 18 14:27:36.984 CST: AAA/AUTHOR/TAC+: (3820424789): send AV service=shell
Feb 18 14:27:36.984 CST: AAA/AUTHOR/TAC+: (3820424789): send AV cmd*
Feb 18 14:27:37.184 CST: AAA/AUTHOR (3820424789): Post authorization status =
PASS_ADD
Feb 18 14:27:37.184 CST: AAA/AUTHOR/EXEC: Authorization successful
```

AAA server `csuslog` output:

```
Feb 18 14:27:36 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful;
[NAS = 172.22.255.3, Port = tty3, User = rtr_techie, Priv = 1]
Feb 18 14:27:36 coachella CiscoSecure: DEBUG -
Feb 18 14:27:36 coachella CiscoSecure: DEBUG - AUTHORIZATION request (e3b70e55)
Feb 18 14:27:36 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd*
output: ]
```

2. User `rtr_techie` enters `enable` mode.

Router **debug** output:

```
Feb 18 14:27:39.776 CST: AAA/MEMORY: free_user (0x61F5DEC0) user='' ruser=''
port='tty3' rem_addr='172.22.53.201' authen_type=ASCII service=ENABLE priv=15
Feb 18 14:27:43.976 CST: tty3 AAA/AUTHOR/CMD (438698848): Port='tty3' list=''
service=CMD
```

3. User *rtr_techie* is denied the **debug all** command.Router **debug** output:

```
Feb 18 14:27:43.976 CST: AAA/AUTHOR/CMD: tty3 (438698848) user='rtr_techie'
Feb 18 14:27:43.976 CST: tty3 AAA/AUTHOR/CMD (438698848): send AV service=shell
Feb 18 14:27:43.976 CST: tty3 AAA/AUTHOR/CMD (438698848): send AV cmd=debug
Feb 18 14:27:43.976 CST: tty3 AAA/AUTHOR/CMD (438698848): send AV cmd-arg=all
Feb 18 14:27:43.976 CST: tty3 AAA/AUTHOR/CMD (438698848): send AV cmd-arg=<cr>
Feb 18 14:27:43.976 CST: tty3 AAA/AUTHOR/CMD (438698848): found list "default"
Feb 18 14:27:43.976 CST: tty3 AAA/AUTHOR/CMD (438698848): Method=tacacs+ (tacacs+)
Feb 18 14:27:43.976 CST: AAA/AUTHOR/TAC+: (438698848): user=rtr_techie
Feb 18 14:27:43.980 CST: AAA/AUTHOR/TAC+: (438698848): send AV service=shell
Feb 18 14:27:43.980 CST: AAA/AUTHOR/TAC+: (438698848): send AV cmd=debug
Feb 18 14:27:43.980 CST: AAA/AUTHOR/TAC+: (438698848): send AV cmd-arg=all
Feb 18 14:27:43.980 CST: AAA/AUTHOR/TAC+: (438698848): send AV cmd-arg=<cr>
Feb 18 14:27:44.180 CST: AAA/AUTHOR (438698848): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 14:27:43 coachella CiscoSecure: DEBUG - AUTHORIZATION request (1a260360)
Feb 18 14:27:43 coachella CiscoSecure: DEBUG - Authorization - Failed command line;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=debug
cmd-arg=all cmd-arg=<cr> output: ]
```

4. User *rtr_techie* is permitted **debug ip packet** command.Router **debug** output:

```
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): Port='tty3'
list='service=CMD'
Feb 18 14:27:47.668 CST: AAA/AUTHOR/CMD: tty3 (3962222355) user='rtr_techie'
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): send AV service=shell
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): send AV cmd=debug
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): send AV cmd-arg=ip
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): send AV cmd-arg=packet
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): send AV cmd-arg=<cr>
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): found list "default"
Feb 18 14:27:47.668 CST: tty3 AAA/AUTHOR/CMD (3962222355): Method=tacacs+ (tacacs+)
Feb 18 14:27:47.668 CST: AAA/AUTHOR/TAC+: (3962222355): user=rtr_techie
Feb 18 14:27:47.668 CST: AAA/AUTHOR/TAC+: (3962222355): send AV service=shell
Feb 18 14:27:47.668 CST: AAA/AUTHOR/TAC+: (3962222355): send AV cmd=debug
Feb 18 14:27:47.668 CST: AAA/AUTHOR/TAC+: (3962222355): send AV cmd-arg=ip
Feb 18 14:27:47.668 CST: AAA/AUTHOR/TAC+: (3962222355): send AV cmd-arg=packet
Feb 18 14:27:47.668 CST: AAA/AUTHOR/TAC+: (3962222355): send AV cmd-arg=<cr>
Feb 18 14:27:47.872 CST: AAA/AUTHOR (3962222355): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 18 14:27:47 coachella CiscoSecure: DEBUG - AUTHORIZATION request (ec2ab713)
Feb 18 14:27:47 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=debug
cmd-arg=ip cmd-arg=packet cmd-arg=<cr> output: ]
```

5. User *rtr_techie* is permitted **clear ip cache** command.Router **debug** output:

```
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): Port='tty3' list=''
service=CMD
Feb 18 14:27:51.760 CST: AAA/AUTHOR/CMD: tty3 (1013999614) user='rtr_techie'
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): send AV service=shell
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): send AV cmd=clear
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): send AV cmd-arg=ip
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): send AV cmd-arg=cache
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): send AV cmd-arg=<cr>
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): found list "default"
Feb 18 14:27:51.760 CST: tty3 AAA/AUTHOR/CMD (1013999614): Method=tacacs+ (tacacs+)
Feb 18 14:27:51.760 CST: AAA/AUTHOR/TAC+: (1013999614): user=rtr_techie
Feb 18 14:27:51.760 CST: AAA/AUTHOR/TAC+: (1013999614): send AV service=shell
Feb 18 14:27:51.760 CST: AAA/AUTHOR/TAC+: (1013999614): send AV cmd=clear
Feb 18 14:27:51.760 CST: AAA/AUTHOR/TAC+: (1013999614): send AV cmd-arg=ip
Feb 18 14:27:51.760 CST: AAA/AUTHOR/TAC+: (1013999614): send AV cmd-arg=cache
Feb 18 14:27:51.760 CST: AAA/AUTHOR/TAC+: (1013999614): send AV cmd-arg=<cr>
Feb 18 14:27:51.964 CST: AAA/AUTHOR (1013999614): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 18 14:27:51 coachella CiscoSecure: DEBUG - AUTHORIZATION request (3c7067fe)
Feb 18 14:27:51 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=clear
cmd-arg=ip cmd-arg=cache cmd-arg=<cr> output: ]
```

6. User *rtr_techie* is denied **reload** command.Router **debug** output:

```
Feb 18 14:27:54.548 CST: tty3 AAA/AUTHOR/CMD (2672654626): Port='tty3' list=''
service=CMD
Feb 18 14:27:54.548 CST: AAA/AUTHOR/CMD: tty3 (2672654626) user='rtr_techie'
Feb 18 14:27:54.548 CST: tty3 AAA/AUTHOR/CMD (2672654626): send AV service=shell
Feb 18 14:27:54.548 CST: tty3 AAA/AUTHOR/CMD (2672654626): send AV cmd=reload
Feb 18 14:27:54.548 CST: tty3 AAA/AUTHOR/CMD (2672654626): send AV cmd-arg=<cr>
Feb 18 14:27:54.548 CST: tty3 AAA/AUTHOR/CMD (2672654626): found list "default"
Feb 18 14:27:54.548 CST: tty3 AAA/AUTHOR/CMD (2672654626): Method=tacacs+ (tacacs+)
Feb 18 14:27:54.548 CST: AAA/AUTHOR/TAC+: (2672654626): user=rtr_techie
Feb 18 14:27:54.548 CST: AAA/AUTHOR/TAC+: (2672654626): send AV service=shell
Feb 18 14:27:54.548 CST: AAA/AUTHOR/TAC+: (2672654626): send AV cmd=reload
Feb 18 14:27:54.548 CST: AAA/AUTHOR/TAC+: (2672654626): send AV cmd-arg=<cr>
Feb 18 14:27:54.752 CST: AAA/AUTHOR (2672654626): Post authorization status = FAIL
```

AAA server *csuslog* output:

```
Feb 18 14:27:54 coachella CiscoSecure: DEBUG - AUTHORIZATION request (9f4d7922)
Feb 18 14:27:54 coachella CiscoSecure: DEBUG - Authorization - Failed command line;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=reload
cmd-arg=<cr> output: ]
```

7. User *rtr_techie* is permitted **show running-config** command.Router **debug** output:

```
Feb 18 14:27:57.576 CST: tty3 AAA/AUTHOR/CMD (3919120170): Port='tty3' list=''
service=CMD
Feb 18 14:27:57.576 CST: AAA/AUTHOR/CMD: tty3 (3919120170) user='rtr_techie'
Feb 18 14:27:57.576 CST: tty3 AAA/AUTHOR/CMD (3919120170): send AV service=shell
Feb 18 14:27:57.576 CST: tty3 AAA/AUTHOR/CMD (3919120170): send AV cmd=show
Feb 18 14:27:57.576 CST: tty3 AAA/AUTHOR/CMD (3919120170): send AV
cmd-arg=running-config
Feb 18 14:27:57.576 CST: tty3 AAA/AUTHOR/CMD (3919120170): send AV cmd-arg=<cr>
Feb 18 14:27:57.576 CST: tty3 AAA/AUTHOR/CMD (3919120170): found list "default"
Feb 18 14:27:57.576 CST: tty3 AAA/AUTHOR/CMD (3919120170): Method=tacacs+ (tacacs+)
Feb 18 14:27:57.576 CST: AAA/AUTHOR/TAC+: (3919120170): user=rtr_techie
Feb 18 14:27:57.576 CST: AAA/AUTHOR/TAC+: (3919120170): send AV service=shell
Feb 18 14:27:57.576 CST: AAA/AUTHOR/TAC+: (3919120170): send AV cmd=show
Feb 18 14:27:57.576 CST: AAA/AUTHOR/TAC+: (3919120170): send AV
cmd-arg=running-config
Feb 18 14:27:57.576 CST: AAA/AUTHOR/TAC+: (3919120170): send AV cmd-arg=<cr>
Feb 18 14:27:57.780 CST: AAA/AUTHOR (3919120170): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 18 14:27:57 coachella CiscoSecure: DEBUG - AUTHORIZATION request (e999072a)
Feb 18 14:27:57 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=show
cmd-arg=running-config cmd-arg=<cr> output: ]
```

8. User *rtr_techie* is permitted **write terminal** command.Router **debug** output:

```
Feb 18 14:28:00.825 CST: tty3 AAA/AUTHOR/CMD (1409504713): Port='tty3' list=''
service=CMD
Feb 18 14:28:00.825 CST: AAA/AUTHOR/CMD: tty3 (1409504713) user='rtr_techie'
Feb 18 14:28:00.825 CST: tty3 AAA/AUTHOR/CMD (1409504713): send AV service=shell
Feb 18 14:28:00.825 CST: tty3 AAA/AUTHOR/CMD (1409504713): send AV cmd=write
Feb 18 14:28:00.825 CST: tty3 AAA/AUTHOR/CMD (1409504713): send AV cmd-arg=terminal
Feb 18 14:28:00.825 CST: tty3 AAA/AUTHOR/CMD (1409504713): send AV cmd-arg=<cr>
Feb 18 14:28:00.825 CST: tty3 AAA/AUTHOR/CMD (1409504713): found list "default"
Feb 18 14:28:00.825 CST: tty3 AAA/AUTHOR/CMD (1409504713): Method=tacacs+ (tacacs+)
Feb 18 14:28:00.825 CST: AAA/AUTHOR/TAC+: (1409504713): user=rtr_techie
Feb 18 14:28:00.825 CST: AAA/AUTHOR/TAC+: (1409504713): send AV service=shell
Feb 18 14:28:00.825 CST: AAA/AUTHOR/TAC+: (1409504713): send AV cmd=write
Feb 18 14:28:00.825 CST: AAA/AUTHOR/TAC+: (1409504713): send AV cmd-arg=terminal
Feb 18 14:28:00.825 CST: AAA/AUTHOR/TAC+: (1409504713): send AV cmd-arg=<cr>
Feb 18 14:28:01.025 CST: AAA/AUTHOR (1409504713): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 18 14:28:00 coachella CiscoSecure: DEBUG - AUTHORIZATION request (540355c9)
Feb 18 14:28:00 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=write
cmd-arg=terminal cmd-arg=<cr> output: ]
```

9. User *rtr_techie* is permitted **copy running-config starting config** command.

Router **debug** output:

```
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): Port='tty3' list=''
service=CMD
Feb 18 14:28:05.269 CST: AAA/AUTHOR/CMD: tty3 (4281070087) user='rtr_techie'
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): send AV service=shell
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): send AV cmd=copy
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): send AV
cmd-arg=running-config
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): send AV
cmd-arg=startup-config
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): send AV cmd-arg=<cr>
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): found list "default"
Feb 18 14:28:05.269 CST: tty3 AAA/AUTHOR/CMD (4281070087): Method=tacacs+ (tacacs+)
Feb 18 14:28:05.269 CST: AAA/AUTHOR/TAC+: (4281070087): user=rtr_techie
Feb 18 14:28:05.269 CST: AAA/AUTHOR/TAC+: (4281070087): send AV service=shell
Feb 18 14:28:05.269 CST: AAA/AUTHOR/TAC+: (4281070087): send AV cmd=copy
Feb 18 14:28:05.269 CST: AAA/AUTHOR/TAC+: (4281070087): send AV
cmd-arg=running-config
Feb 18 14:28:05.269 CST: AAA/AUTHOR/TAC+: (4281070087): send AV
cmd-arg=startup-config
Feb 18 14:28:05.269 CST: AAA/AUTHOR/TAC+: (4281070087): send AV cmd-arg=<cr>
Feb 18 14:28:05.473 CST: AAA/AUTHOR (4281070087): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 18 14:28:05 coachella CiscoSecure: DEBUG - AUTHORIZATION request (ff2bf207)
Feb 18 14:28:05 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=copy
cmd-arg=running-config cmd-arg=startup-config cmd-arg=<cr> output: ]
```

10. User *rtr_techie* is permitted **write memory** command.

Router **debug** output:

```
Feb 18 14:28:08.121 CST: tty3 AAA/AUTHOR/CMD (192752980): Port='tty3' list=''
service=CMD
Feb 18 14:28:08.121 CST: AAA/AUTHOR/CMD: tty3 (192752980) user='rtr_techie'
Feb 18 14:28:08.121 CST: tty3 AAA/AUTHOR/CMD (192752980): send AV service=shell
Feb 18 14:28:08.121 CST: tty3 AAA/AUTHOR/CMD (192752980): send AV cmd=write
Feb 18 14:28:08.121 CST: tty3 AAA/AUTHOR/CMD (192752980): send AV cmd-arg=memory
Feb 18 14:28:08.121 CST: tty3 AAA/AUTHOR/CMD (192752980): send AV cmd-arg=<cr>
Feb 18 14:28:08.121 CST: tty3 AAA/AUTHOR/CMD (192752980): found list "default"
Feb 18 14:28:08.121 CST: tty3 AAA/AUTHOR/CMD (192752980): Method=tacacs+ (tacacs+)
Feb 18 14:28:08.121 CST: AAA/AUTHOR/TAC+: (192752980): user=rtr_techie
Feb 18 14:28:08.121 CST: AAA/AUTHOR/TAC+: (192752980): send AV service=shell
Feb 18 14:28:08.121 CST: AAA/AUTHOR/TAC+: (192752980): send AV cmd=write
Feb 18 14:28:08.121 CST: AAA/AUTHOR/TAC+: (192752980): send AV cmd-arg=memory
Feb 18 14:28:08.121 CST: AAA/AUTHOR/TAC+: (192752980): send AV cmd-arg=<cr>
Feb 18 14:28:08.325 CST: AAA/AUTHOR (192752980): Post authorization status = PASS_ADD
```

AAA server *csuslog* output:

```
Feb 18 14:28:08 coachella CiscoSecure: DEBUG - AUTHORIZATION request (b7d2d54)
Feb 18 14:28:08 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell cmd=write
cmd-arg=memory cmd-arg=<cr> output: ]
```

11. User `rtr_techie` is denied **configure terminal** command.

Router **debug** output:

```
Feb 18 14:28:11.621 CST: tty3 AAA/AUTHOR/CMD (3042655042): Port='tty3' list=''
service=CMD
Feb 18 14:28:11.621 CST: AAA/AUTHOR/CMD: tty3 (3042655042) user='rtr_techie'
Feb 18 14:28:11.621 CST: tty3 AAA/AUTHOR/CMD (3042655042): send AV service=shell
Feb 18 14:28:11.621 CST: tty3 AAA/AUTHOR/CMD (3042655042): send AV cmd=configure
Feb 18 14:28:11.621 CST: tty3 AAA/AUTHOR/CMD (3042655042): send AV cmd-arg=terminal
Feb 18 14:28:11.621 CST: tty3 AAA/AUTHOR/CMD (3042655042): send AV cmd-arg=<cr>
Feb 18 14:28:11.621 CST: tty3 AAA/AUTHOR/CMD (3042655042): found list "default"
Feb 18 14:28:11.621 CST: tty3 AAA/AUTHOR/CMD (3042655042): Method=tacacs+ (tacacs+)
Feb 18 14:28:11.621 CST: AAA/AUTHOR/TAC+: (3042655042): user=rtr_techie
Feb 18 14:28:11.621 CST: AAA/AUTHOR/TAC+: (3042655042): send AV service=shell
Feb 18 14:28:11.621 CST: AAA/AUTHOR/TAC+: (3042655042): send AV cmd=configure
Feb 18 14:28:11.621 CST: AAA/AUTHOR/TAC+: (3042655042): send AV cmd-arg=terminal
Feb 18 14:28:11.621 CST: AAA/AUTHOR/TAC+: (3042655042): send AV cmd-arg=<cr>
Feb 18 14:28:11.825 CST: AAA/AUTHOR (3042655042): Post authorization status = FAIL
```

AAA server `csuslog` output:

```
Feb 18 14:28:11 coachella CiscoSecure: DEBUG - AUTHORIZATION request (b55b3b42)
Feb 18 14:28:11 coachella CiscoSecure: DEBUG - Authorization - Failed command line;
[NAS = 172.22.255.3, user = rtr_techie, port = tty3, input: service=shell
cmd=configure cmd-arg=terminal cmd-arg=<cr> output: ]
```

C.6.3 Test Results for `rtr_super` Group

Tests results follow for each of the Cisco IOS commands summarized in Table 4-1, including relevant router output and AAA server log output:

1. User `rtr_geek` is authorized EXEC shell access.
2. User `rtr_geek` enters enable mode.
3. User `rtr_geek` is denied debug all command.
4. User `rtr_geek` is permitted debug ip packet command.
5. User `rtr_geek` is permitted reload command.
6. User `rtr_geek` is permitted show running-config command.
7. User `rtr_geek` is permitted write terminal command.
8. User `rtr_geek` is permitted copy running-config startup-config command.
9. User `rtr_geek` is permitted write memory command.
10. User `rtr_geek` is permitted configure terminal 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_geek* is authorized EXEC shell access.

Router **debug** output:

```
Feb 22 15:26:16.322 CST: AAA/AUTHOR/TAC+: (424410682): user=rtr_geek
Feb 22 15:26:16.322 CST: AAA/AUTHOR/TAC+: (424410682): send AV service=shell
Feb 22 15:26:16.322 CST: AAA/AUTHOR/TAC+: (424410682): send AV cmd*
Feb 22 15:26:16.822 CST: AAA/AUTHOR (424410682): Post authorization status = PASS_ADD
Feb 22 15:26:16.822 CST: AAA/AUTHOR/EXEC: Authorization successful
Feb 22 15:26:16.822 CST: AAA/ACCT/EXEC/START User rtr_geek, port tty3
Feb 22 15:26:16.822 CST: AAA/ACCT/EXEC: Found list "default"
Feb 22 15:26:16.822 CST: AAA/ACCT/EXEC/START User rtr_geek, Port tty3,
task_id=310 start_time=951254776 timezone=CST service=shell
Feb 22 15:26:16.822 CST: AAA/ACCT: user rtr_geek, acct type 0 (2751112696):
Method=tacacs+ (tacacs+)
Feb 22 15:26:17.022 CST: TAC+: (2751112696): received acct response status = SUCCESS
```

AAA server *csuslog* output:

```
Feb 22 15:26:16 coachella CiscoSecure: DEBUG - Authentication - LOGIN successful;
[NAS = 172.22.255.3, Port = tty3, User = rtr_geek, Priv = 1]
Feb 22 15:26:16 coachella CiscoSecure: DEBUG -
Feb 22 15:26:16 coachella CiscoSecure: INFO - Profile: user = rtr_geek {
Feb 22 15:26:16 coachella set server current-failed-logins = 0
Feb 22 15:26:16 coachella profile_cycle = 2
Feb 22 15:26:16 coachella }
Feb 22 15:26:16 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd*output: ]
```

2. User *rtr_geek* enters **enable** mode.

Router **debug** output:

```
Feb 22 15:26:22.562 CST: AAA/MEMORY: free_user (0x61F55834) user='' ruser=''
port='tty3' rem_addr='172.22.53.201' authen type=ASCII service=ENABLE priv=15
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): Port='tty3' list=''
service=CMD
```

3. User *rtr_geek* is denied **debug all** command.

Router **debug** output:

```
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): Port='tty3' list=''
service=CMD
Feb 22 15:26:46.502 CST: AAA/AUTHOR/CMD: tty3 (32101230) user='rtr_geek'
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): send AV service=shell
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): send AV cmd=debug
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): send AV cmd-arg=all
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): send AV cmd-arg=<cr>
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): found list "default"
Feb 22 15:26:46.502 CST: tty3 AAA/AUTHOR/CMD (32101230): Method=tacacs+ (tacacs+)
Feb 22 15:26:46.502 CST: AAA/AUTHOR/TAC+: (32101230): user=rtr_geek
Feb 22 15:26:46.502 CST: AAA/AUTHOR/TAC+: (32101230): send AV service=shell
Feb 22 15:26:46.502 CST: AAA/AUTHOR/TAC+: (32101230): send AV cmd=debug
Feb 22 15:26:46.502 CST: AAA/AUTHOR/TAC+: (32101230): send AV cmd-arg=all
Feb 22 15:26:46.502 CST: AAA/AUTHOR/TAC+: (32101230): send AV cmd-arg=<cr>
Feb 22 15:26:46.702 CST: AAA/AUTHOR (32101230): Post authorization status = FAIL
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): Port='tty3' list=''
service=CMD
```

AAA server *csuslog* output:

```
Feb 22 15:26:46 coachella CiscoSecure: DEBUG - AUTHORIZATION request (1e9d36e)
Feb 22 15:26:46 coachella CiscoSecure: DEBUG - Authorization - Failed command line;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=debug
cmd-arg=all cmd-arg=<cr> output: ]
```

4. User *rtr_geek* is permitted **debug ip packet** command.

Router **debug** output:

```
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): Port='tty3'
list=' 'service=CMD
Feb 22 15:26:53.378 CST: AAA/AUTHOR/CMD: tty3 (1642620731) user='rtr_geek'
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): send AV service=shell
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): send AV cmd=debug
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): send AV cmd-arg=ip
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): send AV cmd-arg=packet
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): send AV cmd-arg=<cr>
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): found list "default"
Feb 22 15:26:53.378 CST: tty3 AAA/AUTHOR/CMD (1642620731): Method=tacacs+ (tacacs+)
Feb 22 15:26:53.378 CST: AAA/AUTHOR/TAC+: (1642620731): user=rtr_geek
Feb 22 15:26:53.378 CST: AAA/AUTHOR/TAC+: (1642620731): send AV service=shell
Feb 22 15:26:53.378 CST: AAA/AUTHOR/TAC+: (1642620731): send AV cmd=debug
Feb 22 15:26:53.378 CST: AAA/AUTHOR/TAC+: (1642620731): send AV cmd-arg=ip
Feb 22 15:26:53.378 CST: AAA/AUTHOR/TAC+: (1642620731): send AV cmd-arg=packet
Feb 22 15:26:53.378 CST: AAA/AUTHOR/TAC+: (1642620731): send AV cmd-arg=<cr>
Feb 22 15:26:53.578 CST: AAA/AUTHOR (1642620731): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 22 15:26:53 coachella CiscoSecure: DEBUG - AUTHORIZATION request (61e8673b)
Feb 22 15:26:53 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=debug
cmd-arg=ip cmd-arg=packet cmd-arg=<cr> output: ]
```

5. User *rtr_geek* is permitted **reload** command.



Note Be sure to save your running configuration by using the appropriate **write** or **copy running-config** command before using the **reload** command.

Router **debug** output:

```
Feb 22 15:27:16.667 CST: tty3 AAA/AUTHOR/CMD (3461622395): Port='tty3'
list=' 'service=CMD
Feb 22 15:27:16.667 CST: AAA/AUTHOR/CMD: tty3 (3461622395) user='rtr_geek'
Feb 22 15:27:16.667 CST: tty3 AAA/AUTHOR/CMD (3461622395): send AV service=shell
Feb 22 15:27:16.667 CST: tty3 AAA/AUTHOR/CMD (3461622395): send AV cmd=reload
Feb 22 15:27:16.667 CST: tty3 AAA/AUTHOR/CMD (3461622395): send AV cmd-arg=<cr>
Feb 22 15:27:16.667 CST: tty3 AAA/AUTHOR/CMD (3461622395): found list "default"
Feb 22 15:27:16.667 CST: tty3 AAA/AUTHOR/CMD (3461622395): Method=tacacs+ (tacacs+)
Feb 22 15:27:16.667 CST: AAA/AUTHOR/TAC+: (3461622395): user=rtr_geek
Feb 22 15:27:16.667 CST: AAA/AUTHOR/TAC+: (3461622395): send AV service=shell
Feb 22 15:27:16.667 CST: AAA/AUTHOR/TAC+: (3461622395): send AV cmd=reload
Feb 22 15:27:16.667 CST: AAA/AUTHOR/TAC+: (3461622395): send AV cmd-arg=<cr>
Feb 22 15:27:16.867 CST: AAA/AUTHOR (3461622395): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 22 15:27:16 coachella CiscoSecure: DEBUG - AUTHORIZATION request (ce542a7b)
Feb 22 15:27:16 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=reload
cmd-arg=<cr> output: ]
```

6. User *rtr_geek* is permitted **show running-config** command.

Router **debug** output:

```
Feb 22 15:27:34.455 CST: tty3 AAA/AUTHOR/CMD (150984379): Port='tty3' list=''
service=CMD
Feb 22 15:27:34.455 CST: AAA/AUTHOR/CMD: tty3 (150984379) user='rtr_geek'
Feb 22 15:27:34.455 CST: tty3 AAA/AUTHOR/CMD (150984379): send AV service=shell
Feb 22 15:27:34.455 CST: tty3 AAA/AUTHOR/CMD (150984379): send AV cmd=show
Feb 22 15:27:34.455 CST: tty3 AAA/AUTHOR/CMD (150984379): send AV
cmd-arg=running-config
Feb 22 15:27:34.455 CST: tty3 AAA/AUTHOR/CMD (150984379): send AV cmd-arg=<cr>
Feb 22 15:27:34.455 CST: tty3 AAA/AUTHOR/CMD (150984379): found list "default"
Feb 22 15:27:34.455 CST: tty3 AAA/AUTHOR/CMD (150984379): Method=tacacs+ (tacacs+)
Feb 22 15:27:34.455 CST: AAA/AUTHOR/TAC+: (150984379): user=rtr_geek
Feb 22 15:27:34.455 CST: AAA/AUTHOR/TAC+: (150984379): send AV service=shell
Feb 22 15:27:34.455 CST: AAA/AUTHOR/TAC+: (150984379): send AV cmd=show
Feb 22 15:27:34.455 CST: AAA/AUTHOR/TAC+: (150984379): send AV cmd-arg=running-config
Feb 22 15:27:34.455 CST: AAA/AUTHOR/TAC+: (150984379): send AV cmd-arg=<cr>
Feb 22 15:27:34.655 CST: AAA/AUTHOR (150984379): Post authorization status = PASS_ADD
```

AAA server *csuslog* output:

```
Feb 22 15:27:34 coachella CiscoSecure: DEBUG - AUTHORIZATION request (8ffd6bb)
Feb 22 15:27:34 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=show
cmd-arg=running-config cmd-arg=<cr> output: ]
```

7. User *rtr_geek* is permitted **write terminal** command.

Router **debug** output:

```
Feb 22 15:27:39.871 CST: tty3 AAA/AUTHOR/CMD (3013136481): Port='tty3' list=''
service=CMD
Feb 22 15:27:39.871 CST: AAA/AUTHOR/CMD: tty3 (3013136481) user='rtr_geek'
Feb 22 15:27:39.871 CST: tty3 AAA/AUTHOR/CMD (3013136481): send AV service=shell
Feb 22 15:27:39.871 CST: tty3 AAA/AUTHOR/CMD (3013136481): send AV cmd=write
Feb 22 15:27:39.871 CST: tty3 AAA/AUTHOR/CMD (3013136481): send AV cmd-arg=terminal
Feb 22 15:27:39.871 CST: tty3 AAA/AUTHOR/CMD (3013136481): send AV cmd-arg=<cr>
Feb 22 15:27:39.871 CST: tty3 AAA/AUTHOR/CMD (3013136481): found list "default"
Feb 22 15:27:39.871 CST: tty3 AAA/AUTHOR/CMD (3013136481): Method=tacacs+ (tacacs+)
Feb 22 15:27:39.871 CST: AAA/AUTHOR/TAC+: (3013136481): user=rtr_geek
Feb 22 15:27:39.871 CST: AAA/AUTHOR/TAC+: (3013136481): send AV service=shell
Feb 22 15:27:39.871 CST: AAA/AUTHOR/TAC+: (3013136481): send AV cmd=write
Feb 22 15:27:39.871 CST: AAA/AUTHOR/TAC+: (3013136481): send AV cmd-arg=terminal
Feb 22 15:27:39.871 CST: AAA/AUTHOR/TAC+: (3013136481): send AV cmd-arg=<cr>
Feb 22 15:27:40.075 CST: AAA/AUTHOR (3013136481): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 22 15:27:39 coachella CiscoSecure: DEBUG - AUTHORIZATION request (b398d061)
Feb 22 15:27:39 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=write
cmd-arg=terminal cmd-arg=<cr> output: ]
```

8. User *rtr_geek* is permitted **copy running-config startup-config** command.

Router **debug** output:

```
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): Port='tty3'
list=''service=CMD
Feb 22 15:27:44.755 CST: AAA/AUTHOR/CMD: tty3 (2463024765) user='rtr_geek'
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): send AV service=shell
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): send AV cmd=copy
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): send AV
cmd-arg=running-config
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): send AV
cmd-arg=startup-config
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): send AV cmd-arg=<cr>
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): found list "default"
Feb 22 15:27:44.755 CST: tty3 AAA/AUTHOR/CMD (2463024765): Method=tacacs+ (tacacs+)
Feb 22 15:27:44.755 CST: AAA/AUTHOR/TAC+: (2463024765): user=rtr_geek
Feb 22 15:27:44.755 CST: AAA/AUTHOR/TAC+: (2463024765): send AV service=shell
Feb 22 15:27:44.755 CST: AAA/AUTHOR/TAC+: (2463024765): send AV cmd=copy
Feb 22 15:27:44.755 CST: AAA/AUTHOR/TAC+: (2463024765): send AV
cmd-arg=running-config
Feb 22 15:27:44.755 CST: AAA/AUTHOR/TAC+: (2463024765): send AV
cmd-arg=startup-config
Feb 22 15:27:44.755 CST: AAA/AUTHOR/TAC+: (2463024765): send AV cmd-arg=<cr>
Feb 22 15:27:44.959 CST: AAA/AUTHOR (2463024765): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 22 15:27:44 coachella CiscoSecure: DEBUG - AUTHORIZATION request (92cec67d)
Feb 22 15:27:44 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=copy
cmd-arg=running-config cmd-arg=startup-config cmd-arg=<cr> output: ]
```

9. User *rtr_geek* is permitted **write memory** command.

Router **debug** output:

```
Feb 22 15:27:52.351 CST: tty3 AAA/AUTHOR/CMD (3171189379): Port='tty3' list=''
service=CMD
Feb 22 15:27:52.351 CST: AAA/AUTHOR/CMD: tty3 (3171189379) user='rtr_geek'
Feb 22 15:27:52.351 CST: tty3 AAA/AUTHOR/CMD (3171189379): send AV service=shell
Feb 22 15:27:52.351 CST: tty3 AAA/AUTHOR/CMD (3171189379): send AV cmd=write
Feb 22 15:27:52.351 CST: tty3 AAA/AUTHOR/CMD (3171189379): send AV cmd-arg=memory
Feb 22 15:27:52.351 CST: tty3 AAA/AUTHOR/CMD (3171189379): send AV cmd-arg=<cr>
Feb 22 15:27:52.351 CST: tty3 AAA/AUTHOR/CMD (3171189379): found list "default"
Feb 22 15:27:52.351 CST: tty3 AAA/AUTHOR/CMD (3171189379): Method=tacacs+ (tacacs+)
Feb 22 15:27:52.351 CST: AAA/AUTHOR/TAC+: (3171189379): user=rtr_geek
Feb 22 15:27:52.351 CST: AAA/AUTHOR/TAC+: (3171189379): send AV service=shell
Feb 22 15:27:52.351 CST: AAA/AUTHOR/TAC+: (3171189379): send AV cmd=write
Feb 22 15:27:52.351 CST: AAA/AUTHOR/TAC+: (3171189379): send AV cmd-arg=memory
Feb 22 15:27:52.351 CST: AAA/AUTHOR/TAC+: (3171189379): send AV cmd-arg=<cr>
Feb 22 15:27:52.555 CST: AAA/AUTHOR (3171189379): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 22 15:27:52 coachella CiscoSecure: DEBUG - AUTHORIZATION request (bd048283)
Feb 22 15:27:52 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=write
cmd-arg=memory cmd-arg=<cr> output: ]
```

10. User *rtr_geek* is permitted **configure terminal** command.

Router **debug** output:

```
Feb 22 15:27:56.039 CST: tty3 AAA/AUTHOR/CMD (4076778320): Port='tty3' list=''
service=CMD
Feb 22 15:27:56.039 CST: AAA/AUTHOR/CMD: tty3 (4076778320) user='rtr_geek'
Feb 22 15:27:56.039 CST: tty3 AAA/AUTHOR/CMD (4076778320): send AV service=shell
Feb 22 15:27:56.039 CST: tty3 AAA/AUTHOR/CMD (4076778320): send AV cmd=configure
Feb 22 15:27:56.039 CST: tty3 AAA/AUTHOR/CMD (4076778320): send AV cmd-arg=terminal
Feb 22 15:27:56.039 CST: tty3 AAA/AUTHOR/CMD (4076778320): send AV cmd-arg=<cr>
Feb 22 15:27:56.039 CST: tty3 AAA/AUTHOR/CMD (4076778320): found list "default"
Feb 22 15:27:56.039 CST: tty3 AAA/AUTHOR/CMD (4076778320): Method=tacacs+ (tacacs+)
Feb 22 15:27:56.039 CST: AAA/AUTHOR/TAC+: (4076778320): user=rtr_geek
Feb 22 15:27:56.039 CST: AAA/AUTHOR/TAC+: (4076778320): send AV service=shell
Feb 22 15:27:56.039 CST: AAA/AUTHOR/TAC+: (4076778320): send AV cmd=configure
Feb 22 15:27:56.039 CST: AAA/AUTHOR/TAC+: (4076778320): send AV cmd-arg=terminal
Feb 22 15:27:56.039 CST: AAA/AUTHOR/TAC+: (4076778320): send AV cmd-arg=<cr>
Feb 22 15:27:56.239 CST: AAA/AUTHOR (4076778320): Post authorization status =
PASS_ADD
```

AAA server *csuslog* output:

```
Feb 22 15:27:56 coachella CiscoSecure: DEBUG - AUTHORIZATION request (f2feb350)
Feb 22 15:27:56 coachella CiscoSecure: DEBUG - Authorization - Request authorized;
[NAS = 172.22.255.3, user = rtr_geek, port = tty3, input: service=shell cmd=configure
cmd-arg=terminal cmd-arg=<cr> output: ]
```

