

For this lab section, refer to Figure 26-5 on page 922 of the book.

R8 Radius Configuration

```
username user1 privilege 7 password 7 121A0C041104
!
aaa new-model
!
aaa authentication login default group radius local
aaa authentication login no_login local none
aaa authorization exec default local
aaa accounting exec default start-stop group radius
ip radius source-interface loopback 8
!
line con 0
  privilege level 15
  login authentication no_login
!
privilege configure level 7 snmp-server
privilege configure level 7 snmp-server host
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
radius-server host 192.168.1.7 auth-port 1645 acct-port 1646
radius-server key cisco
```

Troubleshooting Commands

```
R8#debug radius authentication
R8#debug radius brief
R8#debug aaa authentication
```

```
R8#sho debugging
General OS:
  AAA Authentication debugging is on
  Radius protocol debugging is on
  Radius protocol brief debugging is on
```

```
R8#
03:20:10: AAA/AUTHEN/LOGIN (0000000D): Pick method list
'default'
03:20:10: RADIUS/ENCODE(0000000D): ask "Username: "
03:20:10: RADIUS/ENCODE(0000000D): send packet; GET_USER
03:20:14: RADIUS/ENCODE(0000000D): ask "Password: "
03:20:14: RADIUS/ENCODE(0000000D): send packet; GET_PASSWORD
03:20:15: RADIUS(0000000D): Storing nasport 68 in rad_db
03:20:15: RADIUS: Pick NAS IP for uid=13 tableid=0
cfg_addr=8.8.8.8 best_addr=0.0.0.0
03:20:15: RADIUS(0000000D): Send Access-Request to
192.168.1.7:1645 id 14, len 76
03:20:15: RADIUS: Received from id 21645/14
192.168.1.7:1645, Access-Accept, len 54
03:20:19: AAA: parse name=tty68 idb type=-1 tty=-1
03:20:19: AAA: name=tty68 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=68 channel=0
```

```
03:20:19: AAA/MEMORY: create_user (0x82F7EE44) user='user1'
ruser='NULL' ds0=0 port='tty68' rem_addr='192.168.1.1'
authen
type=ASCII service=ENABLE priv=15 initial_task_id='0', vrf=
(id=0)
03:20:19: AAA/AUTHEN/START (3095283584): port='tty68'
list='' action=LOGIN service=ENABLE
03:20:19: AAA/AUTHEN/START (3095283584): non-console enable
- default to enable password
03:20:19: AAA/AUTHEN/START (3095283584): Method=ENABLE
03:20:19: AAA/AUTHEN(3095283584): Status=GETPASS
03:20:20: AAA/AUTHEN/CONT (3095283584): continue_login
(user='(undef)')
03:20:20: AAA/AUTHEN(3095283584): Status=GETPASS
03:20:20: AAA/AUTHEN/CONT (3095283584): Method=ENABLE
03:20:20: AAA/AUTHEN(3095283584): Status=PASS
03:20:20: AAA/MEMORY: free_user (0x82F7EE44) user='NULL'
ruser='NULL' port='tty68' rem_addr='192.168.1.1'
authen_type=ASCII
I service=ENABLE priv=15 vrf= (id=0)
```


RADIUS Configuration

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://127.0.0.1:1150/ Go Links



User Setup

User: user1

☐ Account Disabled

Supplementary User Info ?

Real Name

Description

User Setup ?

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

☒ Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

Done Internet

Start acs Untitled - Notepad CiscoSecure ACS ... C:\WINNT\System... Document - WordPad 9:53 PM

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://127.0.0.1:1150/ Go Links

Cisco Systems Group Setup

Jump To Access Restrictions

IETF RADIUS Attributes

- ☒ [006] Service-Type Login
- ☐ [007] Framed-Protocol PPP
- ☐ [009] Framed-IP-Netmask 0.0.0.0
- ☐ [010] Framed-Routing None
- ☐ [011] Filter-Id
- ☐ [012] Framed-MTU (64..65535) 64
- ☐ [013] Framed-Compression None
- ☐ [014] Login-IP-Host

Submit Submit + Restart Cancel

Help

- [Group Settings](#)
- [Voice-over-IP \(VoIP\) Support](#)
- [Default Time-of-Day Access Settings](#)
- [Callback](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Enable Options](#)
- [Token Card Settings](#)
- [Password Aging Rules](#)
- [IP Assignment](#)
- [Downloadable ACLs](#)
- [TACACS+ Settings](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Group Settings

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the

Done

Start acs Untitled - Notepad CiscoSecure ACS ... C:\WINNT\System... Document - WordPad 9:54 PM

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://127.0.0.1:1150/ Go

CISCO SYSTEMS Group Setup

Jump To Access Restrictions [0.0.0.0]

- ☒ [015] Login-Service [Telnet]
- ☐ [016] Login-TCP-Port (0..65535) [0]
- ☐ [018] Reply-Message
- ☐ [020] Callback-Id
- ☐ [022] Framed-Route
- ☐ [023] Framed-IPX-Network
 - ☐ NAS Specifies
 - ☒ Other

Submit Submit + Restart Cancel

Help

- [Group Settings](#)
- [Voice-over-IP \(VoIP\) Support](#)
- [Default Time-of-Day Access Settings](#)
- [Callback](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Enable Options](#)
- [Token Card Settings](#)
- [Password Aging Rules](#)
- [IP Assignment](#)
- [Downloadable ACLs](#)
- [TACACS+ Settings](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Group Settings

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the

Done

Start acs Untitled - Notepad CiscoSecure ACS ... C:\WINNT\System... Document - WordPad 9:54

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://127.0.0.1:1150/ Go Links

Cisco Systems Network Configuration

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

AAA Client Setup For r8

AAA Client IP Address: 8.8.8.8

Key: cisco

Network Device Group: (Not Assigned)

Authenticate Using: RADIUS (Cisco IOS/PIX)

☐ Single Connect TACACS+ AAA Client (Record step in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

Submit Submit + Restart Delete Delete + Restart Cancel

Back to Help

Help

- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Deleting a AAA Client](#)
- [Renaming a AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)

AAA Client IP Address

Type the IP address information for this AAA client.

If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

Done Internet

Start acs Untitled - Notepad CiscoSecure ACS ... C:\WINNT\System... Document - WordPad 9:54 PM

Verify Authorization:

```

R8#debug radius
Radius protocol debugging is on

R8#debug aaa authentication
AAA Authentication debugging is on

R8#debug aaa authorization
AAA Authorization debugging is on

R8#
05:40:08: AAA: parse name=tty66 idb type=-1 tty=-1
05:40:08: AAA: name=tty66 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=66 channel=0
05:40:08: AAA/MEMORY: create_user (0x826ECEF8) user='NULL'
ruser='NULL' ds0=0 port='tty66' rem_addr='192.1
68.1.100' authen_type=ASCII service=LOGIN priv=1
initial_task_id='0'

```

```
05:40:08: AAA/AUTHEN/START (1008895964): port='tty66'
list='' action=LOGIN service=LOGIN
05:40:08: AAA/AUTHEN/START (1008895964): using "default"
list
05:40:08: AAA/AUTHEN/START (1008895964): Method=radius
(radius)
05:40:08: AAA/AUTHEN (1008895964): status = GETUSER
05:40:12: AAA/AUTHEN/CONT (1008895964): continue_login
(user='(undef)')
05:40:12: AAA/AUTHEN (1008895964): status = GETUSER
05:40:12: AAA/AUTHEN (1008895964): Method=radius (radius)
05:40:12: AAA/AUTHEN (1008895964): status = GETPASS
05:40:13: AAA/AUTHEN/CONT (1008895964): continue_login
(user='user1')
05:40:13: AAA/AUTHEN (1008895964): status = GETPASS
05:40:13: AAA/AUTHEN (1008895964): Method=radius (radius)
05:40:13: RADIUS: ustruct sharecount=1
05:40:13: Radius: radius_port_info() success=1
radius_nas_port=1
05:40:13: RADIUS: added cisco VSA 2 len 5 "tty66"
05:40:13: RADIUS: Initial Transmit tty66 id 73
192.168.1.7:1645, Access-Request, len 97
05:40:13: Attribute 4 6 08080808
05:40:13: Attribute 5 6 00000042
05:40:13: Attribute 26 13 0000000902077474
05:40:13: Attribute 61 6 00000005
05:40:13: Attribute 1 13 75736572
05:40:13: Attribute 31 15 3139322E
05:40:13: Attribute 2 18 DC34997A
05:40:13: RADIUS: Received from id 73 192.168.1.7:1645,
Access-Accept, len 26
05:40:13: Attribute 8 6 FFFFFFFF
05:40:13: RADIUS: saved authorization data for user 826ECEf8
at 826E446C
05:40:13: AAA/AUTHEN (1008895964): status = PASS
05:40:13: tty66 AAA/AUTHOR/EXEC (2776044849): Port='tty66'
list='' service=EXEC
05:40:13: AAA/AUTHOR/EXEC: tty66 (2776044849)
user='user1radius'
05:40:13: tty66 AAA/AUTHOR/EXEC (2776044849): send AV
service=shell
05:40:13: tty66 AAA/AUTHOR/EXEC (2776044849): send AV cmd*
05:40:13: tty66 AAA/AUTHOR/EXEC (2776044849): found list
"default"
05:40:13: tty66 AAA/AUTHOR/EXEC (2776044849): Method=LOCAL
05:40:13: AAA/AUTHOR (2776044849): Post authorization status
= PASS_ADD
05:40:13: AAA/AUTHOR/EXEC: Processing AV service=shell
05:40:13: AAA/AUTHOR/EXEC: Processing AV cmd*
05:40:13: AAA/AUTHOR/EXEC: Processing AV priv-lvl=7
05:40:13: AAA/AUTHOR/EXEC: Authorization successful
05:40:13: RADIUS: ustruct sharecount=3
05:40:13: Radius: radius_port_info() success=1
radius_nas_port=1
05:40:13: RADIUS: added cisco VSA 2 len 5 "tty66"
05:40:13: RADIUS: Initial Transmit tty66 id 74
192.168.1.7:1646, Accounting-Request, len 113
05:40:13: Attribute 4 6 08080808
```



```

05:40:13: Attribute 5 6 00000042
05:40:13: Attribute 26 13 0000000902077474
05:40:13: Attribute 61 6 00000005
05:40:13: Attribute 1 13 75736572
05:40:13: Attribute 31 15 3139322E
05:40:13: Attribute 40 6 00000001
05:40:13: Attribute 45 6 00000001
05:40:13: Attribute 6 6 00000007
05:40:13: Attribute 44 10 30303030
05:40:13: Attribute 41 6 00000000
05:40:13: RADIUS: Received from id 74 192.168.1.7:1646,

```

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://127.0.0.1:1150/ Go Links

Reports and Activity

Reports

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

Select

Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts
- Logged-in Users
- Disabled Accounts
- ACS Backup And Restore
- Administration Audit
- User Password Changes
- ACS Service Monitoring

[Back to Help](#)

Select

[Refresh](#) [Download](#)

RADIUS Accounting active.csv

Date	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Fra
03/05/2003	22:18:20	user1	Radius_Group	192.168.1.8	Stop	00000015	31	NAS Prompt	..
03/05/2003	22:17:49	user1	Radius_Group	192.168.1.8	Start	00000015	..	NAS Prompt	..
03/05/2003	22:17:43	user1	Radius_Group	192.168.1.8	Stop	00000014	102	NAS Prompt	..
03/05/2003	22:16:01	user1	Radius_Group	192.168.1.8	Start	00000014	..	NAS Prompt	..
03/05/2003	22:15:49	user1	Radius_Group	192.168.1.8	Stop	00000013	257	NAS Prompt	..
03/05/2003	22:11:32	user1	Radius_Group	192.168.1.8	Start	00000013	..	NAS Prompt	..
03/05/2003	22:11:27	user1	Radius_Group	192.168.1.8	Stop	00000012	23	NAS Prompt	..
03/05/2003	22:11:03	user1	Radius_Group	192.168.1.8	Start	00000012	..	NAS Prompt	..
03/05/2003	22:10:58	user1	Radius_Group	192.168.1.8	Stop	00000011	40	NAS	..

Start | CiscoSecure ACS ... | aaa - WordPad | C:\WINNT\System3... | Local Area Connection ... | Internet | 10:19 PM

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://127.0.0.1:1150/ Go Links »

Reports and Activity

Select

Reports

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

[TACACS+ Accounting](#)
[TACACS+ Administration](#)
[RADIUS Accounting](#)
[VoIP Accounting](#)
[Passed Authentications](#)
[Failed Attempts](#)
[Logged-in Users](#)
[Disabled Accounts](#)
[ACS Backup And Restore](#)
[Administration Audit](#)
[User Password Changes](#)
[ACS Service Monitoring](#)

Back to Help

User List

Users logged in on all AAA Clients

Date and Time	User	Group	Assigned IP	Port	Source AAA Client	Logged In Via
03/05/2003 22:19:47	user1	Radius_Group (1 users)	none	66	8.8.8.8	8.8.8.8

http://127.0.0.1:1150/reports/setup.exe?action=make_page&page=logged_on_users&make_csv=1&sort_by=1&seq=%seq

Start CiscoSecure ACS ... Document - WordPad C:\WINNT\System3... Local Area Connection ... C:\WINNT\System3... 10:19 PM

Debug

R8#**sho debugging**

General OS:

AAA Authentication debugging is on

AAA Authorization debugging is on

AAA Accounting debugging is on

R8#

03:54:59: AAA/ACCT/EVENT/(00000017): CALL START

03:54:59: Getting session id for NET(00000017) : db=82A913B8

03:54:59: AAA/ACCT(00000000): add node, session 23

03:54:59: AAA/ACCT/NET(00000017): add, count 1

03:54:59: Getting session id for NONE(00000017) :

db=82A913B8

03:54:59: AAA/AUTHEN/LOGIN (00000017): Pick method list

'default'

03:55:03: Getting session id for EXEC(00000017) :

db=82A913B8

```
03:55:03: AAA/AUTHOR (0x17): Pick method list 'default'
03:55:03: AAA/AUTHOR/EXEC(00000017): processing AV cmd=
03:55:03: AAA/AUTHOR/EXEC(00000017): processing AV priv-
lvl=7
03:55:03: AAA/AUTHOR/EXEC(00000017): Authorization
successful
03:55:03: AAA/ACCT/EXEC(00000017): Pick method list
'default'
03:55:03: AAA/ACCT/SETMLIST(00000017): Handle 0, mlist
82F64BC4, Name default
03:55:03: Getting session id for EXEC(00000017) :
db=82A913B8
03:55:03: AAA/ACCT/EXEC(00000017): add, count 2
03:55:03: AAA/ACCT/EVENT/(00000017): EXEC UP
03:55:03: AAA/ACCT/EXEC(00000017): Queueing record is START
03:55:03: AAA/ACCT(00000017): Accouting method=radius
(radius)
03:55:03: AAA/ACCT/EXEC(00000017): START protocol reply PASS
03:55:05: unknown AAA/DISC: 1/"User Request"
03:55:05: unknown AAA/DISC/EXT: 1020/"User Request"
03:55:05: AAA/ACCT/EVENT/(00000017): CALL STOP
03:55:05: AAA/ACCT/CALL STOP(00000017): Sending stop
requests
03:55:05: AAA/ACCT(00000017): Send all stops
03:55:05: AAA/ACCT/EXEC(00000017): STOP
03:55:05: AAA/ACCT/EXEC(00000017): Queueing record is STOP
osr 1
03:55:05: AAA/ACCT/NET(00000017): STOP
03:55:05: AAA/ACCT/NET(00000017): Method list not found
03:55:05: AAA/ACCT/NET(00000017): free_rec, count 1
03:55:05: AAA/ACCT/NET(00000017) reccnt 1, csr TRUE, osr 1
03:55:05: AAA/ACCT(00000017): Accouting method=radius
(radius)
03:55:05: AAA/ACCT/EXEC(00000017): STOP protocol reply PASS
03:55:05: AAA/ACCT/EXEC(00000017): Cleaning up from Callback
osr 0
03:55:05: AAA/ACCT(00000017): del node, session 23
03:55:05: AAA/ACCT/EXEC(00000017): free_rec, count 0
03:55:05: AAA/ACCT/EXEC(00000017) reccnt 0, csr TRUE, osr 0
03:55:05: AAA/ACCT/EXEC(00000017): Last rec in db, intf not
enqueued
```