2 RADIUS Authentication

This chapter describes Remote Authentication Dial-In User Service (RADIUS) authentication, which is one of three types of user authentication services available in the switch. Check Point authentication is described in Chapter 1, "Authentication Services," and Lightweight Directory Access Protocol (LDAP) authentication is described in Chapter 3, "LDAP Authentiation." For information about authentication in general, including how to configure Telnet and AV-Clients, see Chapter 1,"Authentication Services."

RADIUS is a standard authentication and accounting protocol defined in RFC 2138 and RFC 2139. A built-in RADIUS client is available in the switch. Any RADIUS server may be used with the client, but a server that supports Vendor Specific Attributes (VSAs) specified by RFC 2138 is recommended. The Alcatel attributes may include group information, time-of-day, or slot/port restrictions. RADIUS servers that do not support VSAs may be used but will not be able to provide the extended features (such as user authorization) offered by the RADIUS client. Check your RADIUS server documentation to find out if your server supports VSAs.

♦ Important Note ♦

If your server does not support VSAs and you are using the client's single authority mode, you *must* configure attribute 26 on the server with group information. If the server does not support VSAs and you are using multiple authority mode, attribute 26 does not have to be configured. See your server documentation, *RADIUS Server Attributes* on page 2-1, and *Configuring the Authority Mode* on page 2-7.

RADIUS authentication is enabled/disabled in the switch using the **layer2auth** command. The authentication parameters are configured using the commands listed in the Layer 2 User Authentication submenu shown in Chapter 1, "Authentication Services." The RADIUS commands are described in detail in this chapter.

♦ Note ♦

The commands are not case-sensitive. Capitalization in the commands is for ease of reading only.

RADIUS Server Attributes

RADIUS servers and RADIUS accounting servers are configured with particular attributes defined in RFC 2138 and RFC 2139 respectively. The attributes carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. This section describes the attributes and how to configure them on the server.

General Attributes

The following table lists RADIUS server attributes 1–39 and 60–63, their descriptions, and whether the Alcatel RADIUS client in the switch supports them. Attribute 26 is for vendor-specific information and is discussed in *Vendor Specific Attributes (VSAs)* on page 2-3. Attributes 40–59 are used for RADIUS accounting servers and are listed in *RADIUS Accounting Server Attributes* on page 2-4.

RADIUS Attribute	Supported?	Notes
1 User-Name	Yes	Used in access-request and account-request packets
2 User-Password	Yes	—
3 CHAP-Password	No	—
4 NAS-IP-Address	Yes	Sent with every access-request
5 NAS-Port	Yes	Virtual port number sent with access-request and account-request packets. Slot/port information is supplied in attribute 26 (vendor-specific).
6 Service-Type 7 Framed-Protocol 8 Framed-IP-Address 9 Framed-IP-Netmask 10 Framed-Routing 11 Filter-Id 12 Framed-MTU 13 Framed-Compression 14 Login-IP-Host 15 Login-Service 16 Login-TCP-Port	No	These attributes are used for dial-up sessions; not applicable to the RADIUS client in the switch.
17 Unassigned	—	—
18 Reply-Message	Yes	Multiple reply messages are supported, but the length of all the reply messages returned in one access-accept or access-reject packet cannot exceed 256 characters.
19 Callback-Number 20 Callback-Id 21 Unassigned 22 Frame-Route 23 Framed-IPX-Network	No	These attributes are used for dial-up sessions; not applicable to the RADIUS client in the switch.
24 State	Yes	Sent in challenge/response packets.
25 Class	Yes	Used to pass information from the server to the client and passed unchanged to the accounting server as part of the accounting-request packet.
26 Vendor Specific	Yes	See *Vendor Specific Attributes* on page 2-3.
27 Session-Timeout	No	—
28 Idle-Timeout	No	—
29 Termination-Action 30 Called-Station-Id 31 Calling-Station-Id 32 NAS-Identifier 33 Proxy-State 34 Login-LAT-Service 35 Login-LAT-Node 36 Login-LAT-Group 37 Framed-AppleTalk-Link 38 Framed-AppleTalk-Network 39 Framed-AppleTalk-Zone 60 CHAP-Challenge 61 NAS-Port-Type 62 Port-Limit 63 Login-LAT-Port	No	These attributes are used for dial-up sessions; not applicable to the RADIUS client in the switch.

Vendor Specific Attributes (VSAs)

The Alcatel RADIUS client supports attribute 26, which includes a vendor ID and some additional sub-attributes called subtypes. The vendor ID and the subtypes collectively are called Vendor Specific Attributes (VSAs). Alcatel, through partnering arrangements, has included these VSAs in some vendors' RADIUS server configurations.

- If your server *does not* support VSAs, the attribute subtypes cannot be configured. If you are using single authority mode, you must configure attribute 26 with group information. If you are using multiple authority mode, this attribute does not have to be configured unless you want to users to have access to multiple groups.
- If your server *does* support VSAs, the attribute subtypes may be defined in the server's dictionary file. If you are using single authority mode, the first VSA subtype, Alcatel-Auth-Group, must be defined on the server for each authenticated group. Alcatel's vendor ID is 800 (SMI Network Management Private Enterprise Code).

Sub-Attribute	Num	Type	Description	Packet Type
Alcatel-Auth-Group	1	integer	The authenticated group number	access-accept
Alcatel-Slot-Port	2	string	Slot(s)/port(s) valid for the user	access-accept
Alcatel-Time-of-Day	3	string	The time of day valid for the user to authenticate	access-accept
Alcatel-Client-IP-Addr	4	ipaddr	IP address used for Telnet only	acct-accept
Alcatel-Group-Desc	5	string	Description of the authenticated group	acct-accept
Alcatel-Port-Desc	6	string	Description of the port	acct-accept

RADIUS Accounting Server Attributes

The following table lists the additional attributes used for RADIUS accounting servers and whether the Alcatel RADIUS client in the switch supports them.

Accounting Attribute	Supported?	Notes
40 Acct-Status-Type	Yes	Four values should be included in the dictionary file: 1 (acct-start), 2 (acct-stop), 6 (failure), and 7 (acct-on). Start and stop correspond to login/logout. The accounting-on message is sent when the RADIUS client is started. This atribute also includes an accounting-off value, which is not supported.
41 Acct-Delay-Time	No	—
42 Acct-Input-Octets	Yes	Tracked per port.
43 Acct-Output-Octets	Yes	Tracked per port.
44 Acct-Session-Id	Yes	Unique accounting ID (Alcatel uses the client's MAC address)
45 Acct-Authentic	Yes	Indicates how the client is authenticated, 4 (AV-Client) or 5 (Telnet). These values should be included in the dictionary file.
46 Acct-Session-Time	No	The start and stop time for a user's session can be determined from the accounting log.
47 Acct-Input-Packets	Yes	Tracked per port.
48 Acct-Output-Packets	Yes	Tracked per port.
49 Acct-Terminate-Cause	Yes	Indicates how the session was terminated: • 1 user_request—acct-stop messages when user logs out • 2 lost_carrier—timeouts and line drops • 6 admin_reset—user administratively removed • 9 NAS_error—invalid group, user not moved to group • 17 user_error—acct-fail message, usually authentication failure
50 Acct-Multi-Session-Id	No	—
51 Acct-Link-Count	No	Multilink sessions not supported.

Enabling RADIUS Authentication

By default, RADIUS authentication is disabled in the switch. Use the **layer2auth** command (available from the Security menu) to enable RADIUS authentication. Follow the steps here to enable RADIUS authentication.

1. Enter the following command:

   layer2auth

   A screen displays similar to the following:

   ```
   Layer 2 User Authentication is not enabled
   Set authentication type to? (r=RADIUS, l=LDAP): (r)
   ```

2. Enter **r** or press **<Enter>** to select RADIUS as the server type.

   The following prompt displays:

   ```
   Set authentication to: (0=Disabled, 1=Enabled) : (0)
   ```

3. Enter **1** to enable authentication.

   If AMC authentication is enabled in the switch, RADIUS authentication cannot be enabled. Use the **fwconfig** command to disable AMC Authentication and then reboot the switch. For information about the **fwconfig** command, see Chapter 1, "Authentication Services."

   If LDAP authentication is enabled in the switch, it is disabled when you set the authentication type to RADIUS. See Chapter 3, "LDAP Authentication."

RADIUS Authentication UI

When RADIUS authentication is configured in the switch using the **layer2auth** command, the User Authentication menu for RADIUS is available from the Security menu. The **layer2auth** command is described in Chapter 1, "Authentication Services."

To display the RADIUS menu, enter **UserAuth** at the system prompt.

If RADIUS Authentication is enabled, the User Authentication submenu displays as follows:

Command	Layer 2 User Authentication Menu
avlAddresses	Define an authentication router port address
avlsAddresses	Show all of the Authentication router port addresses
avlBanner	Define the authentication port login banner
avlsBanner	Display the Authentication port login banner
avlbootpmode	Configure authentication-specific BOOTP relay parameters
avlsbootpmode	Display authentication-specific BOOTP relay parameters
avldnsname	Configure authentication name for DNS
avlsdnsname	Display authentication name for DNS
avlPorts	Set a port to be a Telnet authenticated port
avlsPorts	Show ports that are Telnet authenticated ports
avlWebPath	Set a path restriction on Authentication web pages
avlsWebPath	Show the path restriction on Authentication web pages
avlDrop	Move a user back to their default group
avlsVersion	Display the version numbers of the user authentication module
avlMode	Set the authentication mode
avlsMode	Show the authentication mode
avlPrompts	Set the authentication prompts
avlsPrompts	Display the authentication prompts
avlAuthTime	Set the user response timeout for authentication
avlsAuthTime	Show the user response timeout
avlR1Chain	Set the single authority chain of radius servers
avlsR1Chain	Show the single authority chain of radius servers
avlRMChain	Set the multiple authority chain of radius servers
avlsRMChain	Show the multiple authority chain of radius servers
avlRadAcct	Set a radius accounting server
avlsRadAcct	Show radius accounting servers
avlRadTries	Set the number of retries of a radius server before giving up
avlsRadtries	Show the max number of radius server retries
avlRadTimeout	Set a time to wait for reply from radius server
avlsRadTimeout	Show time to wait for reply from radius server

Main Interface | File Security | Summary System | VLAN Services | Networking Help

RADIUS-specific commands are described in this chapter. The other commands apply to all authentication services in the switch and are described in Chapter 1, "Authentication Services."

Configuring the Authority Mode

RADIUS servers are configured in one of two modes, *single authority* or *multiple authority*, depending on how the authentication network is set up. Single authority mode uses a single list or chain of servers to poll with authentication requests. Multiple authority mode uses multiple chains of servers, one chain for each authenticated group. Single authority mode is the default.

Single Authority

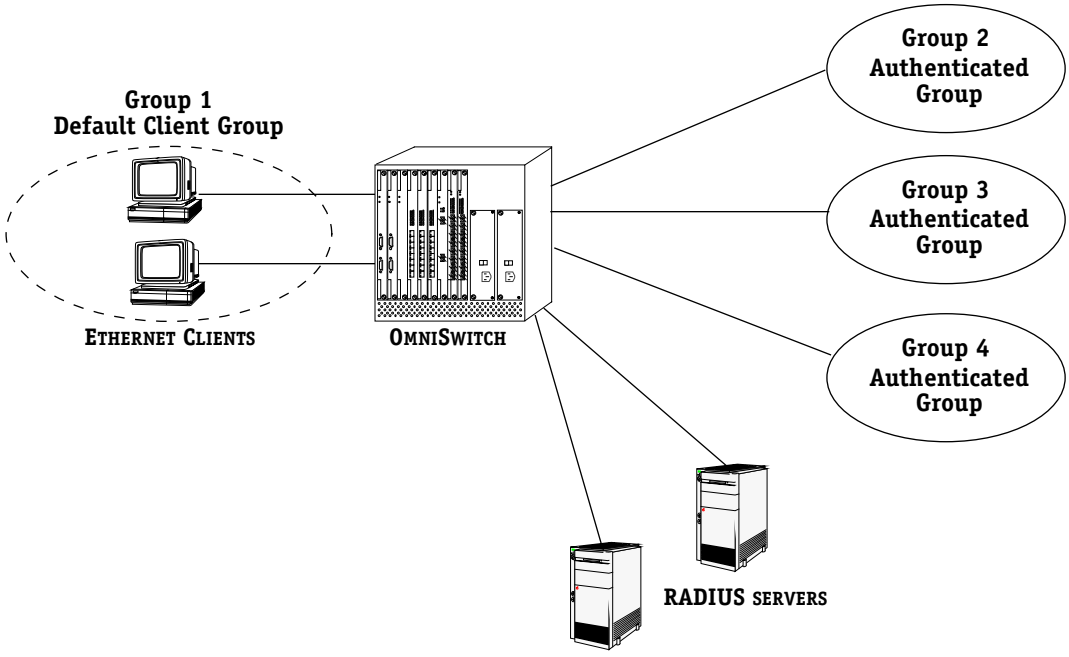
This mode should be used when clients are authenticated using a single server or chain of servers that are configured with group information. When this mode is configured, a client is authenticated into a particular group or groups. (For the client to be authenitcated into multiple groups, each group must be configured for a different protocol.)

When a client first makes a connection to the switch, the agent in the switch polls the RADIUS server(s) for a match with a client's user name and password. When a match is found, the RADIUS server sends a message to the agent in the switch that includes the group IDs to which the client is allowed access. The agent then moves the MAC address of the client out of the default group and into the appropriate authenticated group(s).

♦ Note ♦

If your RADIUS server does not support VSAs, you must configure attribute 26 with group ID information for the clients. See your server documentation for more information.

In the illustration shown here, the Ethernet clients connect to the switch (using the AV-Client or Telnet) and initially belong to group 1, which has been configured on the switch as a mobile group and is the default client group. Additional groups have been configured as authenticated groups. Two RADIUS servers are configured with group ID information for the clients.



RADIUS Authentication Network
Single Authority Mode

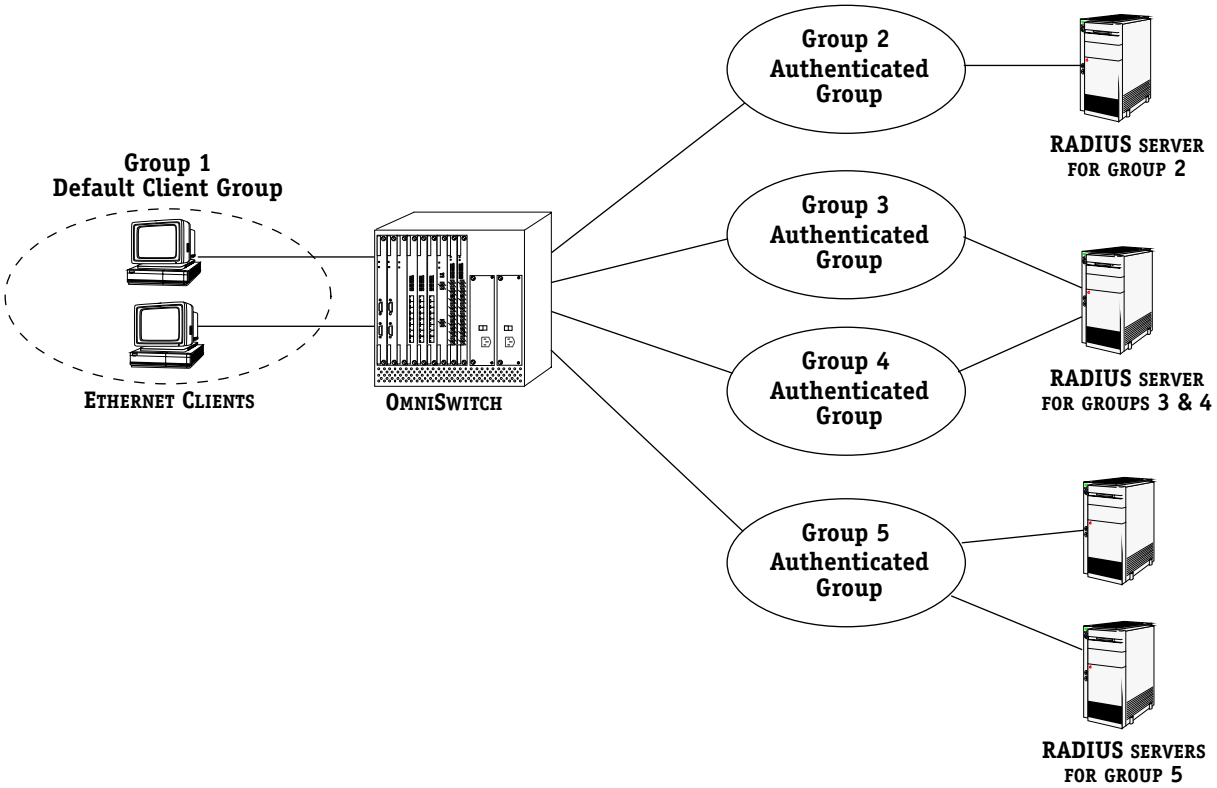
Multiple Authority

Multiple authority mode associates different servers with particular groups. This mode is typically used when one party is providing the network and another is providing the server.

When this mode is configured, a client is first prompted to select a group. After the group is selected, the client then enters a user name and password. The RADIUS server configured for that particular authenticated group is polled for a match. If a match is not found and additional RADIUS servers are configured for the group, they will be polled for the match. When a match is found, the client's MAC address is moved into that group.

The RADIUS server in multiple authority mode does not have to be configured with group information. However, group information may be configured so that clients may have a choice of groups into which they can authenticate. The same user ID and password are used to authenticate into one of several groups. Clients are only able to authenticate into one group at a time. (In single authority mode, clients can authenticate into more than one group at a time if each group is configured for a different protocol.)

In the illustration shown here, the Ethernet clients connect to the switch (using the AV-Client or Telnet) and initially belong to group 1, which has been configured on the switch as a mobile group and is the default client group. Groups 2, 3, 4, and 5 have been configured as authenticated groups. A single RADIUS server is associated with group 2, a chain of two RADIUS servers are associated with group 5; these servers are not configured with group information. Another server is associated with group 3 and group 4; in this case, the server must be configured with group information.



RADIUS Authentication Network
Multiple Authority Mode

Viewing the Current Mode

To view the current mode, enter the following command:

avIsMode

A message similar to the following displays:

the current mode is single authority

Changing the Authority Mode

To change the mode for RADIUS authentication, enter:

avIMode

The following prompt displays:

Set authentication mode to? (1=Single authority, 2=Multiple authority) : () :

Enter the number to select the relevant authority mode. By default the mode is set to single authority.

Servers must be configured for the relevant mode. Servers may also be configured for the mode not in use, but these servers will not be active in the authentication network.

Adding RADIUS Servers

The agent in the switch must be configured to recognize at least one RADIUS server. Multiple servers may be chained together for redundancy. Servers may be configured for both authority modes, but only servers configured for the current mode will be active in the authentication network. The mode may be configured using the **avIMode** command (see *Changing the Authority Mode* on page 2-9).

Adding a RADIUS Server in Single Authority Mode

1. To add a RADIUS server in single authority mode, enter the following command:

   avIR1Chain

   The following prompt displays:

   Do you wish to add or delete a server (add):

2. Press **<Enter>** to add a server. The following prompt displays:

   Radius server IP address: () :

3. Enter the server IP address. The following prompt displays:

   Radius shared secret? ():

   The shared secret is a string of characters known to the switch and to the RADIUS server, but it is not sent out over the network. The secret can be any text string and must be configured here as well as on the server. The secret is case-sensitive.

4. Enter the secret. The following prompt displays:

   Please enter secret once more: () :

5. Enter the secret again. The following prompt displays:

   Server Priority (1{Highest} - 255{Lowest})? (125) :

   The priority indicates the order in which the RADIUS servers are polled with authentication requests. If redundant servers are configured with the same priority, they are polled in the order in which they were added to the chain.

6. Enter the server priority or press **<Enter>** to accept the default. The following prompt displays:

   Radius UDP port number (1645) :

   The UDP port number is determined by the RADIUS server and must be configured here for the switch. This port number is used in IP packets exchanged between the server and switch to indicate that these packets are authentication messages. The UDP port number is 1645 by default. (According to RFC 2138, the UDP port should be 1812, but most RADIUS servers use 1645.) All RADIUS servers in the network may have the same UDP number.

7. Enter the UDP port number or press **<Enter>** to accept the default.

8. Repeat these steps to add additional servers to the chain.

Adding a RADIUS Server in Multiple Authority Mode

At least one authenticated (mobile) group must be configured on the switch in order to add RADIUS servers to a multiple authority chain.

1. To add a RADIUS server in multiple authority mode, enter the following command:

   avlRMChain

   The following prompt displays:

   Do you wish to add or delete a server (add):

2. Press **<Enter>** to add a server. The following prompt displays:

   Authentication Group? () :

3. Enter a mobile group number to which the RADIUS server is attached. (Or enter **0** to indicate all groups.) The following prompt displays:

   Radius server IP address: () :

4. Enter the server IP address. The following prompt displays:

   Radius shared secret? ():

   The shared secret is a string of characters known to the switch and to the RADIUS server, but it is not sent out over the network. The secret can be any text string and must be configured here as well as on the server. The secret is case-sensitive.

5. Enter the secret. The following prompt displays:

   Please enter secret once more: () :

6. Enter the secret again. The following prompt displays:

   Server Priority (1{Highest} - 255{Lowest})? (125) :

   The priority indicates the order in which the RADIUS servers are polled with authentication requests. If redundant servers are configured with the same priority, they are polled in the order in which they were added to the chain.

7. Enter the server priority or press **<Enter>** to accept the default. The following prompt displays:

   Radius UDP port number (1645) :

   The UDP port number is determined by the RADIUS server and must be configured here for the switch. This port number is appended to IP packets exchanged between the server and switch to indicate that these packets are authentication messages. The UDP port number is 1645 by default. (According to RFC 2138, the UDP port should be 1812, but most RADIUS servers use 1645.) All RADIUS servers in the network may have the same UDP number.

8. Enter the UDP port number or press **<Enter>** to accept the default.

9. Repeat these steps to add additional servers to the chain.

Displaying the Authority Chain

A list of RADIUS servers may be displayed for servers in single authority mode or servers in multiple authority mode. The fields are the same on both screens and are described following the screen display examples.

To display the RADIUS servers configured in *single authority mode*, enter the following command:

avlsR1Chain

The screen display is similar to the following:

SERVER	PRIORITY	PORT	GROUP
100.2.1.0	125	1645	0

To display the RADIUS servers configured in *multiple authority mode*, enter the following command:

avlsRMChain

The screen display is similar to the following:

SERVER	PRIORITY	PORT	GROUP
100.1.1.0	125	1645	0

Only one mode is active at a time, but if servers are configured for single authority mode they are also displayed in this list.

These fields are configured using the **avlR1Chain** or **avlRMChain** command and are defined as follows:

Server. The IP address of the RADIUS server.

Priority. Displays the priority of the RADIUS server. When there are multiple servers configured, the priority values determine the order the servers are polled (a value of **1** is the highest priority, a value of **255** is the lowest). If multiple servers are configured with the same priority, they are polled in the order in which they were added to the chain using the **avlR1Chain** or **avlRMChain** command.

Port. Displays the UDP port number. Typically this value is 1645 or 1812.

Group. The number associated with the authenticated group.

Removing RADIUS Servers from a Chain

RADIUS servers may be removed from the chain of servers that are polled with authentication requests. To remove a server you must know the IP address of the server. In addition, if the server is configured in multiple authority mode you must know what authenticated group it belongs to. Use the **avlsR1Chain** and **avlsRMChain** commands to view the current list of servers (see *Displaying the Authority Chain* on page 2-12).

Removing a Server in Single Authority Mode

To remove a RADIUS server from a chain of servers in single authority mode:

1. Enter the following command:

   avlR1Chain

   The following prompt displays:

   Do you wish to add or delete a server (add):

2. Enter **d** and the following prompt displays:

   Radius server IP address: ()

3. Enter the relevant server IP address. The server is removed from the chain of servers configured for the authentication network.

Removing a Server in Multiple Authority Mode

To remove a RADIUS server from a chain of servers in multiple authority mode:

1. Enter the following command:

   avlRMChain

   The following prompt displays:

   Do you wish to add or delete a server (add):

2. Enter **d** and the following prompt displays:

   Authentication Group: ()

3. Enter the relevant authenticated group, and the following prompt displays:

   Radius server IP address: ()

4. Enter the relevant server IP address. The server is removed from the chain of servers configured for the specified group.

Modifying the RADIUS Configuration

You can modify the prompts or messages that display to the client station that is trying to authenticate. You can also set timeouts and the number of retries for authentication attempts.

Configuring RADIUS Agent Prompts/Messages

To modify the RADIUS prompts that display for a user attempting authentication, enter:

```
avlPrompts
```

A screen displays similar to the following:

```
Which prompt do you wish to change:
 g=group
 l=login
 p=password
 c=challenge
 s=success
 f=fail
 t=telnet (logon/logoff): () :
```

Select the prompt by entering the relevant letter. The current message text displays along with a prompt to change the text of the message. For example, if you enter **p**, the screen display is similar to the following

```
The password prompt is:
Password?
Enter message:
():
```

The following describes the prompts/messages in more detail:

group
Prompt that displays for users trying to authenticate to RADIUS servers in multiple authority mode.

login
Prompt that displays for any user trying to authenticate.

password
Prompt that displays for any user trying to authenticate.

challenge
Prompt that displays for users that are required to enter a SecurID or some other token, or use some external device, as part of the authentication process. Whether or not a challenge is required for the authentication process is determined by the type of RADIUS server on which the user is configured.

success
Message that displays when a user is successfully authenticated.

fail
Message that displays when a user cannot be authenticated.

telnet
Prompt that displays for Telnet session logon/logoff.

Displaying the Current Prompts/Messages

To display any of authentication prompts/messages, enter the following command:

```
avIsPrompts
```

A message displays similar to the following:

```
The group prompt is:       Which prompt do you wish to enter?
The logon prompt is:       Login Name?
The password prompt is:    Password?
The challenge prompt is:   Enter challenge response:
The success prompt is:     Authentication Succeeded
The failure prompt is:     Authentication Failed
The Telnet(logon/logoff? prompt is: Connect(1)/Disconnect(2):
```

Use the **avIPrompts** command to configure these prompts/messages. The **avIPrompts** command and the prompts/messages are described in *Configuring RADIUS Agent Prompts/Messages* on page 2-14.

Setting the Timeout for Authentication Attempts

To set the amount of time that must expire before a user can no longer be authenticated because of inactivity during the login process, enter the following command:

```
avIAuthTime
```

The following prompt displays:

```
Set authentication response timeout time (Seconds) : (100) :
```

The current timeout displays at the end of the prompt. Enter the new timeout.

Displaying the Current Timeout for Authentication Attempts

To display the current timeout for authentication attempts, enter the following command:

```
avIsAuthTime
```

A message similar to the following displays:

```
The current authentication user response timeout is 100 seconds
```

Setting the Number of Retries

To set the number of retries the switch makes to the RADIUS server to authenticate a user before trying the next RADIUS server in the list, enter the following command:

```
avIRadTries
```

The following prompt displays:

```
New value for RADIUS server retry attempts: (3) :
```

The current retry attempts value is displayed at the end of the prompt. Enter the new value.

Displaying the Number of Retries

To display the number of retries, enter the following command:

```
avlsRadTries
```

A message similar to the following displays:

```
The current maximum number of retries to a RADIUS server is 3
```

Setting the Timeout for Replies

To configure the timeout for server replies to authentication requests, enter the following command:

```
avlRadTimeout
```

The following prompt displays:

```
Set RADIUS server response timeout time (Seconds): (2) :
```

The current timeout for replies is displayed at the end of the prompt. Enter the desired timeout.

Displaying the Timeout for Replies

To display the timeout for replies, enter the following command:

```
avlsRadTimeout
```

A message similar to the following displays:

```
The current RADIUS server response timeout is 2 seconds
```

Removing a User from an Authenticated Group

To remove a user from an authenticated group, you must first know the user's MAC address. You can find a user's MAC address using the **macinfo** command (see the "Configuring Bridging Parameters" chapter of your switch manual) or in the log files generated by an attached RADIUS accounting server.

When you know the MAC address, enter the following command:

```
avlDrop
```

A message similar to the following displays:

```
Enter MAC address of User: () :
```

Enter the user's MAC address. The user's MAC address is removed from the authenticated group and returned to the default group.

Displaying the Authentication Version

To display the version of the authentication software running on the switch, enter the following command:

```
avlsVersion
```

A message similar to the following displays:

```
Level 2 User Authentication Version 4.1.0.7
```

RADIUS Accounting

RADIUS accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity (when users log in and out, how many login attempts, session length, etc.). The accounting server(s) may be located anywhere in the authentication network.

In single authority mode, the switch will send accounting packets to all configured accounting servers.

In multiple authority mode, the switch must be configured to send accounting packets to the server based on which group the server is associated with. To gather statistics for all groups, configure an accounting server for group 0. To gather statistics for a particular group, configure an accounting server for that group. Multiple accounting servers may be configured for a group or groups for redundancy.

To add a RADIUS accounting server:

1. Enter the following command:

   avlRadAcct

   The following prompt displays:

   Do you wish to add or delete a server (add):

2. Press **<Enter>** to add a server. The next prompt to display depends on whether the switch is configured for single authority or multiple authority mode. If the switch is configured for *multiple authority mode*, the following screen displays:

   If you want to set a default RADIUS accounting server
   for all authenticated groups, choose group 0
   Authentication Group? () :

   To configure a server to gather statistics for all groups, enter **0**. To configure a server for a particular authenticated group, enter the group number.

   If the switch is configured for *single authority mode*, or after entering the group number for a server in multiple authority mode, the following prompt displays:

   Radius server IP address: () :

3. Enter the server IP address. The following prompt displays:

   Radius shared secret? ():

   The shared secret is a string of characters known to the switch and to the RADIUS server, but it is not sent out over the network. The secret can be any text string and must be configured here as well as on the server. The secret is case-sensitive.

4. Enter the secret. The following prompt displays:

   Please enter secret once more: () :

5. Enter the secret again. The following prompt displays:

   Server Priority (1{Highest} - 255{Lowest})? (125) :

   The priority indicates the order in which the RADIUS servers are polled with authentication requests. If more than one server is configured with the same priority, the servers are polled in the order in which they were added to the chain.

6. Enter the server priority or press **<Enter>** to accept the default. The following prompt displays:

   Radius UDP port number (1646) :

   The UDP port number is determined by the RADIUS server and must be configured here for the switch. This port number is appended to IP packets exchanged between the server and switch to indicate that these packets are authentication messages. The UDP port number is 1646 by default. (According to RFC 2139, the UDP port should be 1813, but most RADIUS accounting servers use 1646.) All RADIUS accounting servers in the network may have the same UDP number. Enter the UDP port number or press **<Enter>** to accept the default.

7. Repeat these steps to configure additional accounting servers.

Deleting a RADIUS Accounting Server

To delete a RADIUS accounting server:

1. Enter the following command:

   avlRadAcct

   The following prompt displays:

   Do you wish to add or delete a server (add):

2. Enter **d** to delete the group. The next prompt to display depends on whether the switch is configured for single authority or multiple authority mode. If the switch is configured for *multiple authority mode*, the following prompt displays:

   Authentication Group: ()

   Enter the relevant authenticated group number.

3. If the switch is configured for *single authority mode*, or after specifying the group number of the server in multiple authority mode, the following prompt displays:

   Radius server IP address: ()

4. Enter the relevant server IP address. The server is removed from the chain of servers that gather statistics for the particular group.

Displaying RADIUS Accounting Servers

To display a list of RADIUS accounting servers, enter the following command:

```
avIsRadAcct
```

The screen display is similar to the following:

```
SERVER          PRIORITY        PORT    GROUP
100.2.1.1         125           1646      0
```

These fields are configured using the **avIRadAcct** command and are defined as follows:

Server. The IP address of the RADIUS accounting server.

Priority. The priority of the RADIUS accounting server. When there are multiple servers configured, the priority values determine the order the servers are polled (a value of **1** is the highest priority, a value of **255** is the lowest). If more than one server is configured with the same priority, the servers are polled in the order in which they were added to the chain.

Port. The UDP port number. Typically this value is 1646 or 1813.

Group. The number associated with the authenticated group.