3 LDAP Authentication

Introduction

This chapter describes Lightweight Directory Access Protocol (LDAP) Authentication, one of three user authentication services available in the OmniSwitch, OmniS/R and OmniStack. Check Point Authentication is described in Chapter 1, "Authentication Services", and Remote Authentication Dial-In User Service (RADIUS) is described in Chapter 2, "Radius Authentication".

For information about authentication in general, including how to configure Telnet and Authenticated Clients in Virtual Local Area Networks (AV-Cs), see Chapter 1, "Authentication Services". (IP firewall which is part of the Check Point software is discussed separately in Chapter 4, "IP Firewall").

LDAP Authentication essentially provides the same authentication functions as the Check Point and RADIUS solutions. Although these authentication solutions share many software components, only one service may be used at a time.

LDAP Authentication services use LDAP-enabled directory servers rather than RADIUS servers. The directory servers are used to store usernames, passwords and related information for the LDAP Authentication service in the switch. The service accesses this information to validate and authorize users in the correct mobile group before allowing them network access. LDAP-enabled directory servers must support version 3 of the LDAP protocol. LDAP Authentication includes basic user accounting and logging functions. It also requires host installations of the AV-C and Telnet clients (see *Authentication Clients* on page 3-3.

General Assumptions and Recommendations

Instructions for installing and configuring LDAP-enabled directory servers compatible with an LDAP client in the switch are located in Chapter 8, "IP Control", a feature that uses LDAP technology to provide IP address management functions through the switch. An understanding of LDAP and directory server operations in both features is necessary as LDAP Authentication services used in conjunction with IP Control in the same switch is a supported configuration.

For reference purposes, Chapter 8, "IP Control", contains an in-depth discussion of LDAP technical standards and operations relative to the switch. This information is also applicable to LDAP Authentication services with few exceptions other than the directory schema extensions that apply only to LDAP Authentication services as described in this chapter. Here the focus is mainly on implementing the LDAP Authentication services with the proper schema, and setting the User Interface commands to establish switch communications between the LDAP client providing the authentication services and the LDAP-enabled directory servers.

LDAP Authentication requires that LDAP-enabled primary and secondary servers containing databases of users, passwords and authenticated mobile groups be set up in the network prior to using the feature. *It is strongly recommended* that Chapter 8, "IP Control" be reviewed for guidelines on setting up LDAP-enabled directory servers, if there is no existing LDAP-enabled directory server in use.

Network Administrators can remove users from these mobile groups at anytime via UI command; for more information on setting up groups and VLANs, refer to the chapter on "Configuring Groups and VLAN Policies" in the switch manual. The following is a brief overview of user authentication services in relation to LDAP Authentication.

Note

Group mobility from the default group is a required element of user authentication services in the switch. Because Autotracker VLANs are used for networked devices such as printers, and do not provide group mobility, groups created using Autotracker cannot be used with switch authentication services. (See the chapter on "Managing Autotracker VLANs" in the switch manual.)

Authentication Network Services Overview

Authenticated Networks use authentication clients, agents, and servers. The authentication clients or host workstations communicate with the authentication agent (LDAP client in this instance) on the switch to perform user authentication. The client in the switch presents a text screen during the authentication process through which users log-in to the network. The LDAP Authentication client in the switch uses LDAP-enabled directory servers to store network log-in validation and authorization data for users assigned to authenticated mobile groups.

Authentication Clients

There are two main types of host authentication clients. The first is the Authenticated VLANs client (AV-C) which must be installed with the 32-bit data link protocol (MS DLC 32 UDP.exe file) on workstations in the authentication network. By default AV-C loads when host machines are first booted and startup authentication is performed. AV-C workstation clients may be configured to load or not load automatically at startup. Refer to Chapter 1, "Authentication Services" for instructions on installing the AV-C client.

The second client, the Telnet host authentication client, uses Telnet to perform authentication. After the authentication process is complete, the Telnet sessions end and close. Telnet users must issue Telnet requests to a specific Telnet IP address and port. This pre-configured address can be defined through the **avlAddresses** command for all clients as described in *"Defining Telnet Authentication Port Addresses"* in Chapter 1, "Authentication Services". (The Telnet address may be the same on multiple switches.)

Note

The Telnet authentication port is always 259. In addition to AV-C and Telnet, a Linux client may be used to authenticate. The client supports Linux x86. The client software, a README file, and a network startup/shutdown script example are available on the Internetworking Division FTP site. AV-C is recommended over Telnet as AV-C does not require IP addresses for authenticated groups.

Either client type must be directly connected to the switch or connected via a shared hub, i.e, there cannot be a router between the client and the switch.

How LDAP Authentication Works

The Authenticated VLANs Clients (AV-C) or Telnet interface is accessed from workstations by users to connect to the LDAP switch authentication client via an authenticated port.

When users attempt to log-in, the switch prompts them to enter their username and password. If no matching information is located when the switch queries LDAP-enabled directory servers (in one or more groups depending on the configuration), a user error message is sent. If the username and password match information stored in the directory database, a successful user log-in message is sent and access is granted to the appropriate mobile group from the default client log-in group (which is also mobile).

At this time, the client host is moved from the default log-in group to one or more authenticated groups depending on the user profile stored in the LDAP-enabled directory server. Authenticated groups are mobile groups requiring users to validate rights to access the network. The list of authorized or authenticated groups can be stored in user entries on the directory server or in the directory organization entry that is parent to the user entries in the directory server. See *Directory Server Schema for LDAP Authentication* on page 3-9.

Authentication Agent

The authentication agent is the client software that resides on the MPM in the switch. The agent communicates with the authentication host client and the authentication server to support the authentication process. The authentication client for the Authentication Management Console (AMC) is part of the Firewall client image file, **fwd.img**, and is described in Chapter 1, "Authentication Services".

Likewise, the LDAP Authentication client in the switch is part of the same **rav.img** client image file used for RADIUS Authentication. Although only one method of authentication may be used at a time, authentication networks may alternate between the two (providing the appropriate servers are in use) by enabling the desired method of authentication. This is done via the layer2auth UI command; see *Enabling LDAP Authentication* on page 3-12.

Authentication Servers

The authentication data used by the switch agent performing authentication for users is stored on servers which support server-based authentication procedures. LDAP Authentication specifically requires the use of LDAP-enabled directory servers. For every access attempt, the LDAP authentication client will query the directory server. Log-out messages are cached in the switch until they can be processed by the LDAP switch client, in which case no other information is cached for the user; see *Logging and Accounting Features* on page 3-7. The LDAP authentication log-in and access process applies only to users. LDAP Authentication allows users access to permitted groups without requiring them to enter multiple passwords.

Modes of Operation for Authentication Services

Two different modes of operation are available in the authentication services in the switch, namely the single authority and multiple authority modes. As with RADIUS, LDAP Authentication services run in either single or multiple authority modes. In single authority mode, there is one authentication service or authority for all users, and in the multiple authority mode, there is one authentication service or authority per VLAN group. A detailed discussion of single and multiple authority modes, which is generally applicable to LDAP Authentication servers, is located in Chapter 2, "RADIUS Authentication".

In either mode, the LDAP Authentication provided by the LDAP client in the switch to the servers is the simple, clear text password-based bind. LDAP server and user authentication passwords stored in the switch memory or FLASH are encrypted and non-echoing onscreen.

LDAP Authentication in either mode follows two basic steps by which users gain access to network resources. The first step is authentication which validates a username, and the second is authorization which grants access based on the group membership (rights) associated with the username.

To be authenticated, each user must adhere to the log-in process requiring them to be a member in one or more groups based on their assigned user profile. Once the log-in process is completed and users are approved, they are added to the appropriate group.

Note

There is a default group for users who attempt to log-in to the switch. All users will be assigned into this group before they are authenticated and placed in another group.

Configuring the Authority Mode

To use LDAP Authentication, LDAP-enabled directory servers must be configured in one of two modes, depending on how the authentication network is set up overall. The authority modes for LDAP Authentication are set via UI commands which are accessible once the

rav.img file has been loaded into the switch (refer to "RADIUS Authentication" and "IP Control", Chapters 2 and 8, for information on standard procedure for loading switch image files).

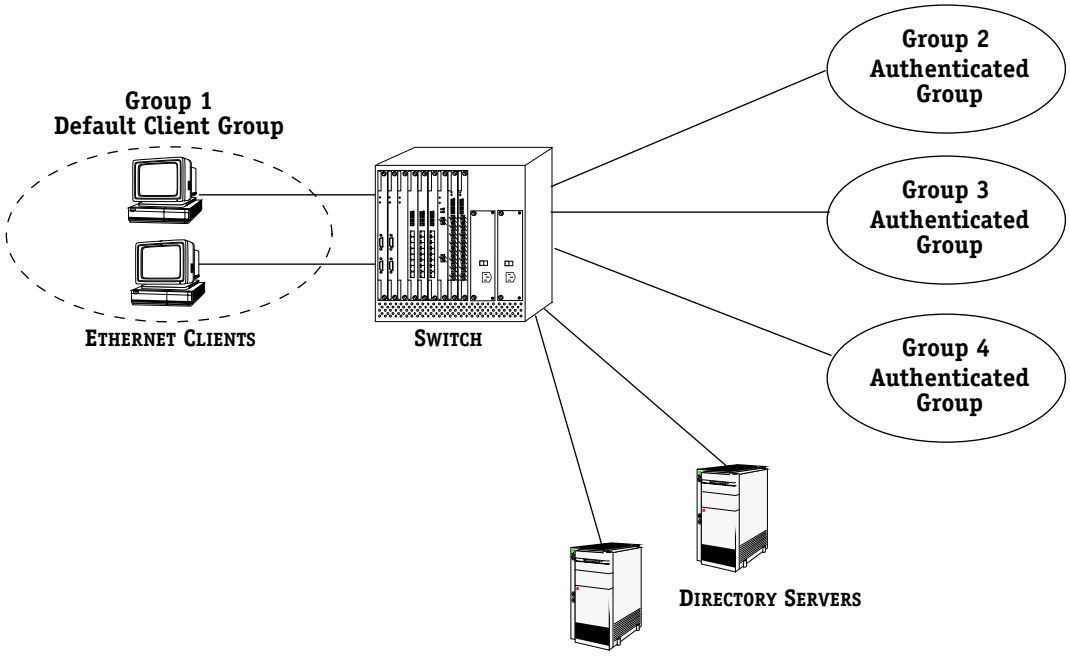
Note

In addition to installing the **rav.img** on the MPM, if the authenticated groups and associated VLANs are not set up in advance through some other service, the individual ports used for VLAN access will need to be configured as authenticated ports. See Chapter 1, "Authentication Services", for details on configuring ports. Authentication ports are limited to modules supporting group mobility.

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 Mode

In the following illustration for Single Authority mode, users connecting to the switch (using Telnet or AV-C) initially belong to group 1 and are configured on the switch as a mobile client group by default. Additional groups have been configured as authenticated groups. Two directory servers are configured with group ID information for the client workstations.



LDAP Authentication Network — Single Authority Mode

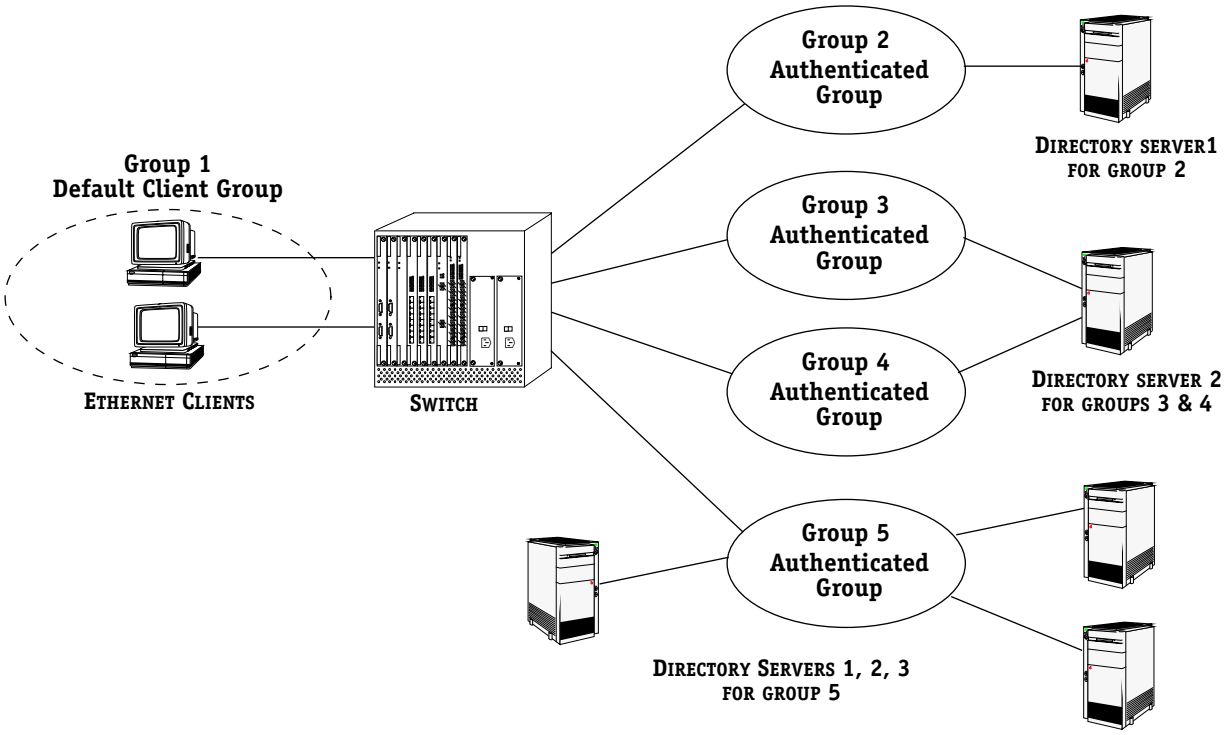
Multiple Authority Mode

In the following illustration for Multiple Authority mode, users connecting to the switch (using Telnet or AV-C) initially belong to group 1 and are configured on the switch as a mobile client group by default.

Groups 2, 3, 4 and 5 have been configured as authenticated groups. A single directory server is associated with group 2, and a chain of three directory servers are associated with group 5. Servers in group 5 are not configured with group information to allow clients a choice of groups into which they can authenticate.

Another server is associated with group 3 and group 4; in this case, the directory server must be configured with group information.

Currently, up to three LDAP-enabled directory servers may be used at one time with the LDAP Authentication service.



LDAP Authentication Network — Multiple Authority Mode

Logging and Accounting Features

The following information is logged in LDAP-enabled directory servers for each authentication user. The features allows users to log-in to multiple groups. The accounting log can be turned ON and OFF via this UI command:

```
/security/userauth % avllschain
```

Refer to the LDAP Authentication UI commands for details on settings (see *LDAP Authentication UI Commands* on page 3-13. Logging and accounting features include Account Start, Stop and Fail Times, and Dynamic Log as follows:

Note

Typically, the Login, Logout and Dynamic logs can be accessed from the directory server software. Each log records the MAC address from the workstation used to log-in to the network. Additional third-party software is required to retrieve and reset the log information to the directory servers for billing purposes.

AccountStartTime

User account start times are tracked in the AccountStartTime attribute of the user's directory entry that keeps the time stamp and accounting information of successful user log-ins. The following fields (separated by carriage returns "|") are contained in the Login log. A different carriage return such as the "#" sign may be used in some situations.

- Client MAC address: xx:xx:xx:xx:xx:xx:xx (mixed characters/digits).
- Time Stamp (YYYYMMDDHHMMSS (YYYY:year, MM:month, DD:day, HH:hour, MM:minute, SS:second)
- Client IP address: variable length digits.
- Switch slot number to which client connects: nn
- Switch port number to which client connects: nn
- Switch virtual number client connects to: nn
- Switch group number client joins in multiple authority mode (0=single authority; 2=multiple authority; variable length digits.
- Switch serial number: xxxxx-xxxxxxxxx (mixed characters/digits).

AccountStopTime

User account stop times are tracked in the AccountStopTime attribute that keeps the time stamp and accounting information of successful user log-outs. The same fields as above (separated by carriage returns "|") are contained in the Logout log. A different carriage return such as the "#" sign may be used in some situations. Additionally, these fields are included but apply only to the Logout log:

- Number of bytes received on the port during the client's session from log-in to log-out: variable length digits.
- Number of bytes sent on the port during the client's session from log-in to log-out: variable length digits.

- Number of frames received on the port during the client's session from log-in to log-out: variable length digits.
- Number of frames sent on the port during the clients session from log-in to log-out: variable length digits.
- Log-out reason code: n

  *0=time-out
  *1=user log-out
  *2=removed by administrator

AccountFailTime

User account fail times are tracked in the AccountFailTime attribute log that keeps the time stamp and accounting information of unsuccessful user log-ins with error codes. The same fields as with the Login Log which are also part of the Logout log (separated by carriage returns "|") are contained in the Login Fail log. A different carriage return such as the "#" sign may be used in some situations. Additionally, these fields are included but apply only to the Login Fail log.

- User account ID or username client entered to log-in: variable length digits.
- User account password client entered for log-in attempt: variable length digits.
- Log-in fail error code: nn. For error codes descriptions refer to the vendor-specific listing for the specific directory server in use.

Dynamic Log

The following dynamic entries are kept in the user's entry in the LDAP-enabled directory server database from the time users successfully log-in and out, at which time the entries are removed.

- switchSerialNumber: switch serial number to which client connected: xxxxx-xxxxxxxxx (mixed characters/digits).
- switchSlotPort: switch slot/port number to which client connected: nn/nn
- clientMACaddress: client MAC address: xx:xx:xx:xx:xx:xx:xx (mixed characters/digits).
- clientIPaddress: variable length digits.

Note

If directory server errors occur during user log-in, the user receives an error message. The log-in attempts will fail and will not be kept in the database, even if switch accounting is turned ON.

If directory server errors occur during user log-out, the Logout log will be stored temporarily if switch accounting is turned ON. The log messages will be transferred to the directory server database when the server recovers. If switch accounting is OFF, only the Dynamic log information is temporarily stored and then transferred.

Directory Server Schema for LDAP Authentication

The LDAP Authentication code is implemented by the LDAP-enabled directory server containing the Lightweight Directory Interchange File (LDIF) server schema extensions required to perform authentication services with LDAP. Server schema extensions should be entered before enabling the feature through the UI commands (see *LDAP Authentication UI Commands* on page 3-13).

The schema is standard and typical of that used for LDAP operations in IP Control as described in Chapter 8. Object classes and attributes will need to be modified accordingly to include LDAP authentication in the network (object classes and attributes are used specifically here to map user account information contained in the directory servers).

LDAP Authentication schema may differ with respect to its inclusion of object classes and attributes that indicate and define password policies. Netscape directory server, for example, requires the following schema be used.

- All LDAP-enabled Netscape directory servers require entry of an auxiliary objectClass:passwordObject for user password policy information.
- Another auxiliary objectClass: password policy is used by the directory server to apply the password policy for the entire server. There is only one entry of this object for the database server.

LDIF files may be imported to directory servers using commands available to a particular server. Refer to Chapter 8, “IP Control” for general instructions on modifying and importing **.ldif** database files, object class (oc) and attribute (at) configuration (**.conf**) files, and/or to the vendor-specific instructions included with the directory server. The above-mentioned files may be included on a distribution CD or possibly downloadable from Alcatel.

Password Policies and Directory Servers

Password policies applied to user accounts vary slightly from one directory server to another. Normally, only the password changing policies can be set by users through the directory server graphical user interface (GUI). Other policies accessible only to Network Administrators through the directory server GUI may include one or more of the following operational parameters.

- Log-in Restrictions
- Change Password
- Check Password Syntax
- Password Minimum Length
- Send Expiration Warnings
- Password History
- Account Lockout
- Reset Password Failure Count
- LDAP Error Messages (e.g., Invalid Username/Password, Server Data Error, etc.)

If using a generic directory server (other than Netscape, Sun, or Novell Directory servers) the switch assumes that the directory server has some mechanism for managing password policies for users; however, the switch does not use these mechanisms to authenticate users.

For instructions on installing LDAP-enabled directory servers, refer to the vendor-specific instructions, and to the example guidelines provided in Chapter 8, “IP Control”, and/or Chapter 6, “Policy Manager, for installing Netscape Directory Server on an NT server.

Schema Extensions for LDAP Authentication

The attributes listed here for user entries extend the object classes in the directory server schema, and are used to manage user accounts. The attributes need to be extended from the default server schema to store user authentication data. Details, example and guidelines for extending LDAP-enabled directory schema are provided in Chapter 8, "IP Control".

accountStartTime	CIS (Case Sensitive String)	
accountStopTime	CIS	
accountFailTime	CIS	
switchSerialNumber	CIS	
switchSlotPort	CIS	
clientMACaddress	CIS	
switchGroups	INT (Integer)	# for single authority mode only
numberOfSwitchGroups	INT (single value)	# for single authority mode only

Note

The attributes switchGroups and numberOfSwitch-Groups are only used in single authority mode. Clients are placed in the group specified during the log-in process in multiple authority mode. Multi-value attributes are used for multiple authority mode.

Schema for LDAP authentication can be extended using a standard text editor as follows.

1. Edit the file that defines attributes and add the additional attributes listed above.
2. Create a new auxiliary object class (Xylan Authentication Person) in the file that can be used to define new objects, e.g., slapd_oc_users.conf for the directory.
3. Add the auxiliary object and new attributes to the entries in the LDIF file that contains the user database.

The attributes switchGroups and numberOfGroups can be associated between the user entries or the immediate parent entries. Group information will be read by the switch at the user level and at the level of the immediate parent group.

Unique User Identifiers

User identifiers must be unique in the entire LDAP database domain, including referral servers. Network Administrators are responsible for the integrity of unique user identifiers whether or not this is enforced through the authentication service or some other tool.

Schema Extensions by Directory Service

Entries for user account authentication schema includes the extensions listed below. These extensions must be included.

- Netscape and Novell Directory Servers (3.0 or later)

  objectClass top
  objectClass person
  objectClass organizational person
  objectClass user

  User account information is stored in the user directory or e-main directory on Netscape Directory Servers.

  Novell Directory Servers store user account information in the same database as the NetWare user account.

- Sun Directory Services (3.1)

  objectClass top
  objectClass account
  objectClass posixAccount (UNIX username)

  Sun Directory Services do not use account or password policies.

Enabling LDAP Authentication

By default, LDAP Authentication is disabled in the switch. Use the **layer2auth** command (available from the Security menu) to enable LDAP Authentication. Follow these steps to enable LDAP Authentication.

Note

If using Check Point Firewall the switch must be rebooted before authentication can be enabled.

If the Authentication Management Console (AMC) authentication is enabled in the switch, LDAP 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".

1. Enter this command:

   layer2auth

   A screen displays similar to the following:

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

2. Enter **l** and press **<Enter>** to select LDAP as the server type.

   If a message displays indicating RADIUS authentication is enabled, enter R to select RADIUS and then disable it by entering **0** when the following prompt displays:

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

   Note

   If RADIUS authentication is enabled in the switch, it must be disabled before the authentication type can be set to LDAP.

   After RADIUS is disabled, re-enter the layer2auth command and set the authentication type to LDAP. Enter 1 when prompted to enable LDAP operations.

LDAP Authentication UI Commands

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

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

If LDAP Authentication is enabled, the following submenu displays (see *Enabling LDAP Authentication* on page 3-12 if it does not display):

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**
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**
avlLSChain	**Set the single authority chain of ldap servers**
avlsLSChain	**Show the single authority chain of ldap servers**
avlLMChain	**Set the multiple authority chain of ldap servers**
avlsLSChain	**Show the multiple authority chain of ldap servers**
avlsVersion	**Display the version numbers of the user authentication module**

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

Most of the commands listed above generally apply to all authentication services included in the switch. These commands are described in Chapter 1,"Authentication Services". The commands which are LDAP-specific, starting with the **avlmode** command, are described in this chapter.

Note to RADIUS users: The LDAP Authentication **layer2auth** menu differs slightly from the RADIUS menu in that the commands for accounting servers, server retries and replies for LDAP Authentication are subset commands of the a**vlLMChain** command in the LDAP **User-Auth** submenu. Also, the set prompts (**avlPrompt**) challenge command does not apply to LDAP Authentication and is included only in the RADIUS prompts menu.

Authentication Mode and Prompts

The operational mode of the authentication service can be viewed and changed as described below.

Viewing the Current Mode

To see whether the current mode for LDAP Authentication is single or multiple authority, enter the following command:

```
avlMode
```

A message similar to the following displays:

```
the current mode is single authority
```

Changing the Authority Mode

To change the mode for LDAP authentication, enter:

```
avlsMode
```

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.

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

Configuring Directory Servers

The prompts or messages that display to the client station trying to authenticate can be modified. Timeouts and number of retries allowed for authentication attempts can also be set as described below.

Configuring Host Client Prompts/Messages

To modify the prompts that display for users attempting authentication through LDAP, enter:

```
avlPrompts
```

A screen displays similar to the following:

```
Which prompt do you wish to change:
 g=group
 l=login
 p=password
 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 any user trying to authenticate in multiple authority mode.

login
Prompt that displays for any user trying to authenticate.

password
Prompt that displays for any user trying to authenticate.

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 the authentication prompts/messages, enter the following command:

```
avlsPrompts
```

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 success prompt is: Indication Succeeded
The failure prompt is: Authentication Failed
The Telnet (logon/logoff? prompt is: Connect (1) / Disconnect (2):
```

Use the **avlPrompts** command above to configure these prompts/messages.

Setting the Timeout for User Authentication Attempts

To set the amount of time that must expire before a user can no longer be authenticated due to inactivity during the log-in process, enter the following command:

```
avlAuthTime
```

The following prompt displays:

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

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

Displaying the Current Timeout for User Authentication Attempts

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

```
avlsAuthTime
```

A message similar to the following displays:

```
The current authentication user response timeout is 50 seconds.
```

Adding, Viewing and Removing Directory Servers

The LDAP switch client must be configured to recognize at least one LDAP-enabled directory server. Multiple servers may be chained together for replication and referral purposes. 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, single or multiple authority, may be configured using the **avlMode** command.

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

Commands used to add directory servers to authentication services are listed below for each mode, and subsequently defined.

Adding Directory Servers (Single or Multiple Authority Mode)

To add directory servers in single authority mode, enter the following command:

avlLSChain

The following prompts display sequentially as an entry is made in each field:

LDAP server super user dn? () :
LDAP super user password: () :
Please enter password once more: () :
LDAP server search base? () :
LDAP server chain () :
LDAP server type to?
(1=Generic Schema, 2=Netscape Directory Server)
(3=Novell NDS, 4=Sun Directory Services) : () :
LDAP server retry attempts: () :
LDAP server response timeout (Seconds) : () :
LDAP server accounting on/off? (1=on, 2=off) : () :
LDAP server login fail log identifier? () :

The following describes prompts in the single authority mode as listed above:

LDAP server super user dn? () :

Enter the super user dn, i.e., the administrative distinguished name recognized by the LDAP-enabled directory servers (e.g., cn=manager)

LDAP super user password: () :

Enter the super user password, i.e., the adminstrative password recognized by LDAP-enabled directory servers (e.g, secret). (This command is followed by a request to re-enter the password, and is used to validate correct password entry.)

LDAP server search base: () :

Enter the search base recognized by LDAP-enabled directory servers (e.g., **o=company, c=US**).

LDAP server chain: () :

Enter the number designating the sequence in which a directory server is accessed in a chain of servers.

As part of the server chain command, a submenu displays requesting entry of the directory server in the format: IPaddress:Port; separate each server by a space; (e.g., 201.11.22.1.389.)

LDAP server type to: () :

Enter the number for the directory server type used in LDAP Authentication:

1=Generic Schema
2=Netscape Directory Server
3=Novell NDS
4=Sun Directory Services

LDAP server retry attempts :() :

Enter the number of retries the switch can make to an LDAP-enabled directory server to authenticate a user before trying the next directory server in the list. Server retry times must be between 1 and 100.

LDAP server response timeout (Seconds) :() :

Enter the number of seconds that must expire before a user can no longer be authenticated due to inactivity during login process. Server timeout time must be between 1 and 90.

LDAP server accounting on/off (1=on, 2=off) : () :

Enter the appropriate number to enable or disable logging and accounting functions for user accounts in the LDAP Authentication service.

LDAP server login fail log identifier? () :

Enter a discretionary identifier to notify users when access to LDAP authentication services is denied due to log-in failure.

Note

Login banners can be modified using the **avlBanner** command (see Chapter 1, "Authentication Services").

To add, edit, or remove directory servers in multiple authority mode, enter the following command:

avlLMChain

The following two additional prompts display sequentially (before the same commands as above for single authority mode) as an entry is made in each field:

Do you wish to add(a), edit(e), or delete(d) a server (a) :
Authentication group? : () :

The following describes prompts in the multiple authority mode as listed above:

Do you wish to add(a), edit(e), or delete(d) a server (a) :

Add, edit or delete a directory server in multiple authority mode by selecting the appropriate letter.

Note

Directory servers may be edited or removed from a chain of servers that are polled with authentication requests once they have been added to the chain. All servers are edited or removed from a chain of servers in multiple authority mode for the authenticated group to which the server belongs. Use the **avlsLSChain** and **avlsLMChain** commands to view list of servers in a chain.

Authentication group? : () :

Enter the mobile group number to which the LDAP-enabled directory server is attached. A group number cannot be entered unless the group has been created (see VLAN management commands accessible from main UI menu).

Viewing the Server Authority Chain (Single or Multiple Authority Mode)

A list of directory servers may be viewed in single or multiple authority mode. The fields are nearly identical in both screens and are described following the screen display examples; the **Authentication group id** only displays in the multiple authority mode. Mode of authority settings cannot be viewed unless the mode is enabled (use the **avlmode** command).

To view directory servers in single authority mode, enter the following command:

```
avlsLSChain
```

The screen display is similar to the following:

```
LDAP server super user dn: cn=directory manager, o-company, c=US
LDAP server search base: o=company, c=US
LDAP server chain: 2
LDAP server type to: Netscape Directory Server
LDAP server retry attempts: 3
LDAP server response timeout (Seconds) : 30
LDAP server accounting: on
LDAP server login fail log identifier: user log-in failed
```

To view directory servers in multiple authority mode, enter the following command:

```
avlsLMChain
```

The screen display is similar to the following:

```
Authentication group id: 2
LDAP server super user dn: cn=directory manager, o=company, c=US
LDAP server search base: o=company, c=US
LDAP server chain: 3
LDAP server type to: Netscape Directory Server
LDAP server retry attempts: 3
LDAP server response timeout (Seconds) : 30
LDAP server accounting: on
LDAP server login fail log identifier: user log-in failed
```

Although only one mode can be active at a time, all configured servers are displayed in the multiple authority list. When there are multiple servers configured, the chain priority value determines 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 using the chain commands.

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 4.0.0.72
```