1 Authentication Services

Introduction

Authentication services provide a high level of security by using group membership to grant access to network resources. Authenticated groups are a special form of mobile group that are associated with a particular protocol or all protocols. These groups include devices that are dynamically assigned based on authentication criteria. Instead of learning group membership based on traffic sent by end systems, authenticated groups control membership through a log-in process (*user authentication*), or through port-binding policies or static port assignment (*device authentication*).

This chapter gives an overview of both user and device authentication and describes configuration procedures for authentication clients. There are three user authentication options in the switch, each requiring a different authentication server—Check Point Authentication Management Console (AMC), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP)-enabled server. This chapter describes how to configure Check Point AMC authentication on the switch. See Chapter 2, "RADIUS Authentication," and Chapter 3, "LDAP Authentication" for specific information about configuring those types of user authentication.

User Authentication

User authentication is based on group mobility, the ability to move a user from one virtual group to another without physically changing ports. Authenticated log-in processes are designed for mobile users and ports that are available to anyone who wants to connect to them. User devices are not tied to a specific switch port since group membership is determined by a user-profile rather than a port location. User authentication is supported for devices attached to Ethernet and Token Ring switch ports. (The AV-Client, however, is only supported on Ethernet interfaces. See *Managing Authentication Clients* on page 1-17 for more information about the AV-Client.)

A default mobile group must be configured to which all authentication switch ports will belong. At least one authenticated group must be configured. When a user connects to the switch, they belong to the default group; after authentication they are moved to the appropriate group or groups.

There are two options for user authentication in the switch: a licensed authentication agent from Check Point Technologies that uses an AMC; or an Alcatel Layer 2 Authentication agent developed for authentication using any RADIUS or LDAP-enabled server. The RADIUS and LDAP solutions offer expanded authorization features. Only one authentication option may be enabled on the switch at one time.

♦ Important Note ♦

User authentication may only be set up for mobile groups. It is not supported on non-mobile groups. However, authenticated groups may exist on the same switch as non-mobile groups and other, non-authenticated mobile groups.

Device Authentication

Device authentication allows a specific device to have access to the network through port-binding policies that compare the device's MAC address and network address or protocol to those configured for the switch port. This type of authentication is designed for non-mobile devices, such as servers, printers, and workstations. Devices may be attached to ports that are statically assigned to authenticated groups. Or devices may gain membership to authenticated groups through port-binding policies. Port-binding policies are most appropriate for devices in physically unsecured areas and are configured like any other AutoTracker policies. The binding policies prevent unauthorized access through the physical port used by the non-mobile device.

Interaction with IP Firewall: *Important Configuration Note*

Authenticated groups and IP Firewall are both methods for increasing the security of a network. Authenticated groups may be set up on the same network as the IP Firewall software but not necessarily on the same switch. RADIUS or LDAP authentication may be enabled on a switch that is running IP Firewall. However, *a single switch cannot run both IP Firewall and Check Point Authentication (AMC) at the same time.* For more information about IP firewall, see Chapter 4, "IP Firewall."

Authentication and DHCP

User authentication is compatible with the Dynamic Host Control Protocol (DHCP). If authentication clients are configured to use DHCP to get their IP addresses, the DHCP server should be defined as part of either the default client group or the authenticated group or both depending on the client you are using and the way the network is set up. There is an integrated DHCP server in the switch that may be used for supplying IP addresses or as a proxy for an external DHCP server. Additional information about DHCP as it relates to authentication is included in this chapter in *Authentication Clients and DHCP* on page 1-31.

Protocol Groups

Because authenticated groups do not support protocol or network address policies, it is difficult to determine the protocol type supported in such a group. When you create an authenticated group using the **crgp** command, you can configure the group to be associated with one protocol or all protocols.

A single device can belong to more than one authenticated group. If the device supports more than one protocol type, such as IP and IPX, then it can belong to multiple authenticated groups, one group per protocol, or it can belong to a single group that supports all protocols.

A device cannot belong to more than one authenticated group associated with the same protocol. For example, if the device meets the criteria for more than one IP-based authenticated group, then it will be assigned to the first configured IP group.

MAC Timeouts

AutoTracker normally ages out MAC devices that have been inactive for a certain period of time. This MAC timeout parameter is configurable through the **stc** command. You may need to configure this parameter for some device in an authenticated network. See the bridging parameters chapter of your switch user manual for more information about the **stc** command.

Components of an Authenticated Network

An authentication network is composed of authentication clients, an authentication agent, and an authentication server. These components are described here and illustrated on the next pages.

Authentication Client

The authentication client communicates with the authentication agent on the switch to perform user authentication. The client presents the text screen through which a user logs in during the authentication process.

There are two types of authentication clients. The first is a proprietary Authenitcated VLAN Client (AV-Client) client, which must be installed on the user's PC. By default the AV-Client loads when the user PC is first booted and performs authentication at startup. The AV-Client may be configured not to automatically load at startup. Note that the AV-Client is scheduled for future release. Contact Alcatel for the latest information about the AV-Client.

The second client uses Telnet to perform authentication. After the authentication process is complete, the Telnet session ends and closes. The Telnet user must issue a Telnet request to a Telnet address and port. This pre-configured address can be defined through the **avlAddresses** command, which is described in *Defining Telnet Authentication Addresses* on page 1-27. (The Telnet address may be the same on multiple switches.) The Telnet authentication port is always 259.

In addition to the AV-Client and Telnet, a Linux client may be used to authenticate. The client supports Linux x86 and is scheduled for future release. Contact Alcatel for the latest client software, README file, and a network startup/shutdown script example.

The AV-Client and Telnet authentication clients are discussed in this chapter.

♦ Note ♦

The client must be directly connected to the switch or connected via a shared hub. There cannot be a router between the client and the switch.

Authentication Agent

This authentication agent is software that resides on the MPM of the switch. This agent communicates with the authentication client, authentication server, and AutoTracker software to support the authentication process. The authentication agent for an AMC is part of the Firewall client image file (**fwd.img**, **fwx.img**, or **fw4.img**). The authentication agent for a RADIUS or LDAP server is provided in the RADIUS/LDAP client image file, **rav.img**.

♦ Important Note ♦

Only one authentication agent may be enabled in the switch at a time.

You can configure AMC agent parameters through the **fwconfig** command, which is described in *Configuring AMC Authentication* on page 1-33. RADIUS authentication agent parameters are configured through the **layer2auth** command and other commands in the Layer 2 User Authentication submenu (see Chapter 2, "RADIUS Authentication").

Authentication Server

The authentication server may be an Authentication Management Console (AMC), a RADIUS server, or an LDAP server. There must be at least one authentication server in a network supporting user-authenticated groups.

An AMC uses Check Point Technologies' proprietary protocol and is a Windows NT station running a software application that contains a database of users, passwords, and authentication methods. The software maintains a secured communication path with the authentication agent in the switch. The AMC may use its native authentication mechanisms, or it may use an attached external third-party solution such as Security Dynamics SecurID, Axent Defender, or RADIUS. The software can reside on the same PC as other network management software, such as Switch Manager, but it cannot reside on the same PC as firewall server software. See the *VLAN Authentication Manager-1 Administrator Guide* for instructions on setting up AMC software.

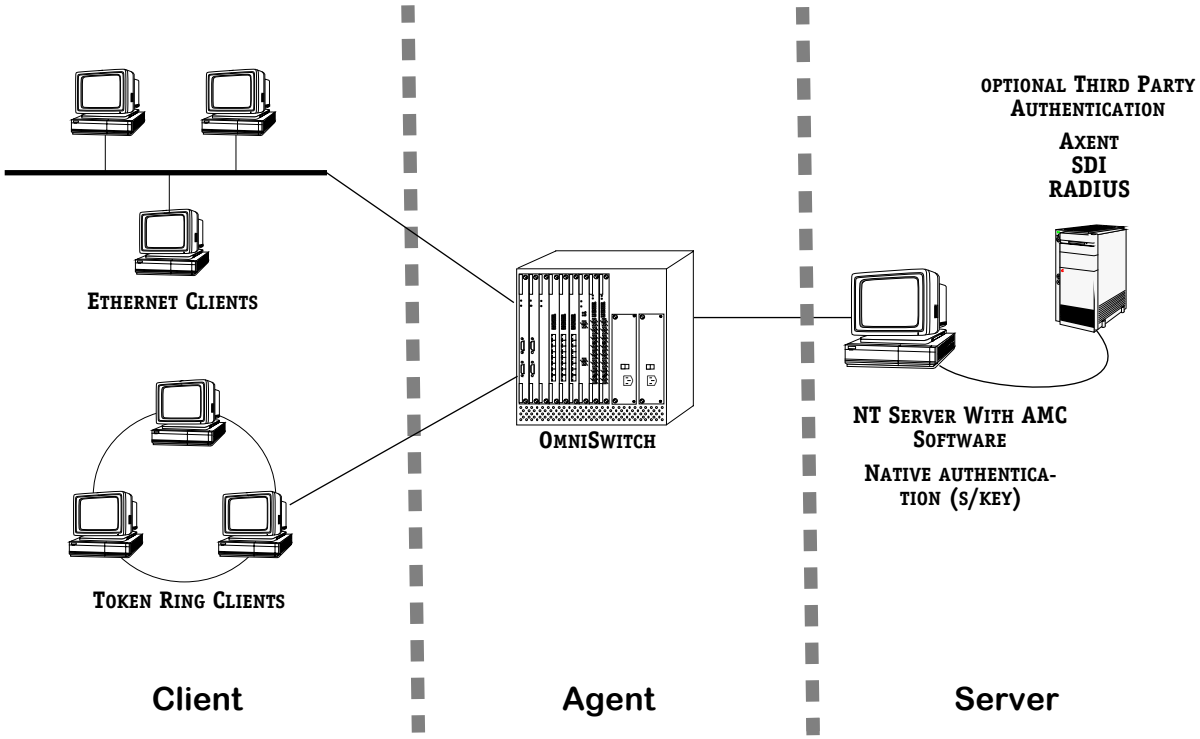
♦ Note ♦

Version 1.1 of the AMC software is Y2K-compliant.
Earlier versions of the software are not Y2K-compliant.

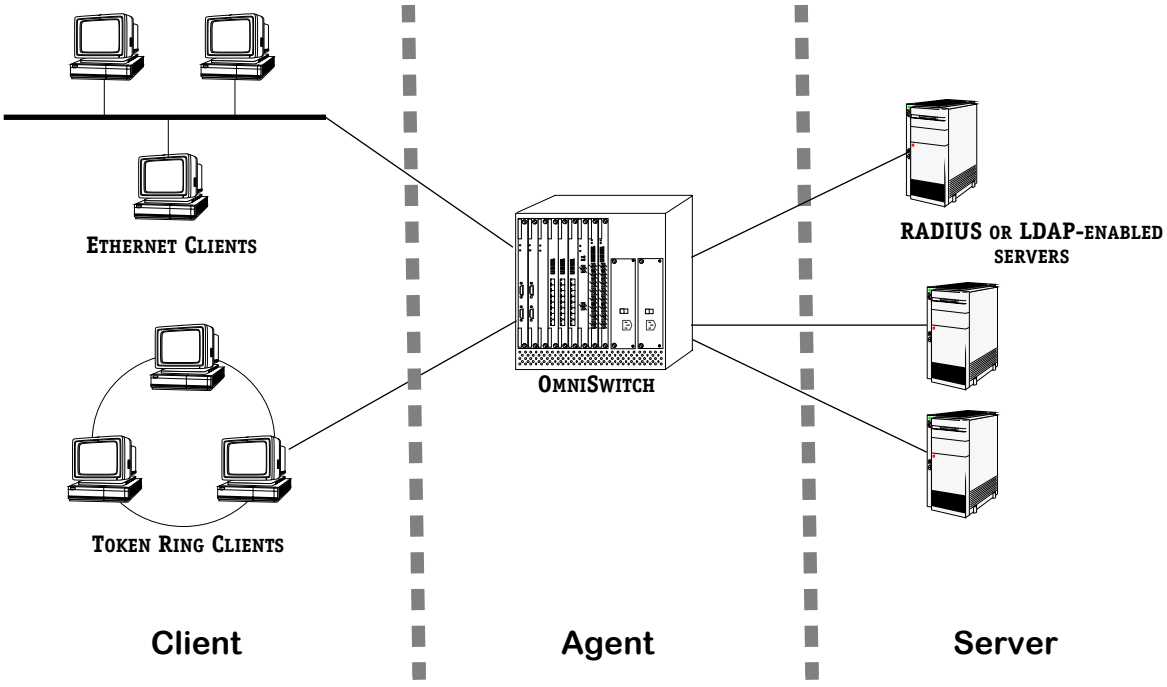
A RADIUS server contains a database of user names and passwords, challenges/responses, and other authentication criteria such as time-of-day access. Multiple RADIUS servers may be configured in the network, and the RADIUS agent in the switch may be configured to poll these servers using one of two different modes, single authority or multiple authority. RADIUS servers may also be configured to use RADIUS accounting software for gathering statistics about the authentication network. See your RADIUS server manufacturer's documentation for information about configuring the server and Chapter 2," RADIUS Authentication."

An LDAP-enabled server is a directory server that contains user information and profiles and may be used for user authentication on the switch. Multiple LDAP-enabled servers may be configured in the network, and the LDAP authentication agent in the switch may be configured to poll these servers using one of two different modes, single authority or multiple authority. See your server manufacturer's documentation for information about configuring the server and Chapter 3, "LDAP Authentication."

The diagrams on the next page illustrate each of these components.



Authentication Network With Check Point AMC



Authentication Network With RADIUS or LDAP Agent and Servers

Configuration Overview

Setting up a network using authentication requires several broad steps. Configuration is required on the switch (where the agent resides), the authentication server, and client stations. The following is a broad outline of the steps involved; each step is covered in more detail in other chapters or later within this chapter.

Step 1. Configure Groups on the Switch

Authentication clients must be connected to ports in a default mobile group and at least one authenticated group must be configured.

- *Configure Group Mobility for the Switch*
  Group mobility must be globally enabled on the switch using the **gmcfg** command. See the "Managing Groups and Ports chapter in your switch user manual for more information about this command.
- *Configure Group Mobility for Default Group*
  By default all ports automatically belong to group 1. When group mobility is enabled globally on the switch, group 1 is automatically configured as a mobile group. If you want a different group to be the default group, you can create a new mobile group through the **crgp** command or change an existing group into a mobile group through the **gmstat** command. Client ports may then be added to that group through the **addvp** command. These commands are described in the "Managing Groups and Ports" chapter of your switch user manual.
- *Create Mobile Groups that Require Authentication*
  Use the **crgp** command to create at least one group with group mobility and authentication enabled. The **crgp** command is described in the "Managing Groups and Ports" chapter of your switch user manual. User authentication is set up by configuring clients and servers and enabling authentication on the switch as described in the next steps.
- *(Optional) Set Up Device Authentication*
  Device authentication may be set up using static ports or port-binding policies.
    - *Add Static Ports*
      In order for a device to gain membership to an authenticated group it must meet certain criteria. You set up this criteria on the switch. One way for a device to gain membership to an authenticated group is simply to attach it to a port that has been statically assigned to the group. You can statically assign ports to an authenticated group through the **crgp** and **addvp** commands. These commands are described in the "Managing Groups and Ports" chapter of your switch user manual.
    - *Set Up Port-Binding Policies*
      Another way for a device to gain membership to an authenticated group is to meet the specifications of a port-binding policy. Port-binding polices require devices to match three criteria. The criteria can be one of two combinations; the device must match all values in the criteria set. The device can attach to a specific switch port *and* use a specific MAC address *and* use a specific protocol (IP or IPX); **or** the device can attach to a specific switch port *and* use a specific MAC address *and* use a specific IP network address. Port-binding policies are described in the "AutoTracker Policies" chapter of your switch user manual.

Step 2. Configure Clients

If you are employing a user login procedure as a basis for membership in an authenticated group, then you need to configure client software. Client software configuration is described in this chapter in *Managing Authentication Clients* on page 1-17.

If you are using the Alcatel proprietary Authenticated VLANs Client (AV-Client), then you need to install this Windows-based software (it operates on Windows 95, Windows 98, and Windows NT) on all workstations that will need to log in. See *Installing AV-Clients* on page 1-19. You must also configure the switch ports that will be used for authentication.

Users can also log in through a Telnet session, which requires a standard Telnet application to be available on user workstations. You must configure router port addresses and switch ports that will be used for Telnet authentication. If the Telnet client will be using a web browser to authenticate, you may want to configure an authentication host name. If the Telnet client will be using DHCP to obtain an IP address, you may need to configure a BOOTP relay interface. See *Setting Up Telnet Clients* on page 1-27.

Step 3. Configure Authentication Server(s)

The authentication server also must be configured. The Check Point AMC runs a Windows NT based software program and its configuration is described in the *VLAN Authentication Manager-1 Administrator Guide*.

For RADIUS servers, refer to the manufacturer's documentation for configuration information. Information about server attributes is included in Chapter 2, "RADIUS Authentication."

For LDAP-enabled servers, refer to the manufacturer's documentation for configuration information as well as Chapter 3, "LDAP Authentication."

Step 4. Configure Authentication on the Switch

Use the User Authentication submenu commands to configure authentication parameters. See *User Authentication UI Commands* on page 1-15.

Configuration specific to the Check Point (AMC) Authentication software in the switch is described in *Configuring AMC Authentication* on page 1-33.

Configuration specific to Layer 2 Authentication (RADIUS or LDAP) is described in Chapter 2, "RADIUS Authentication" and Chapter 3, "LDAP Authentication."

♦ Note ♦

Only one type of authentication software may be enabled in the switch at one time, either Check Point (AMC) Authentication or Layer 2 Authentication (RADIUS *or* LDAP).

Application Example

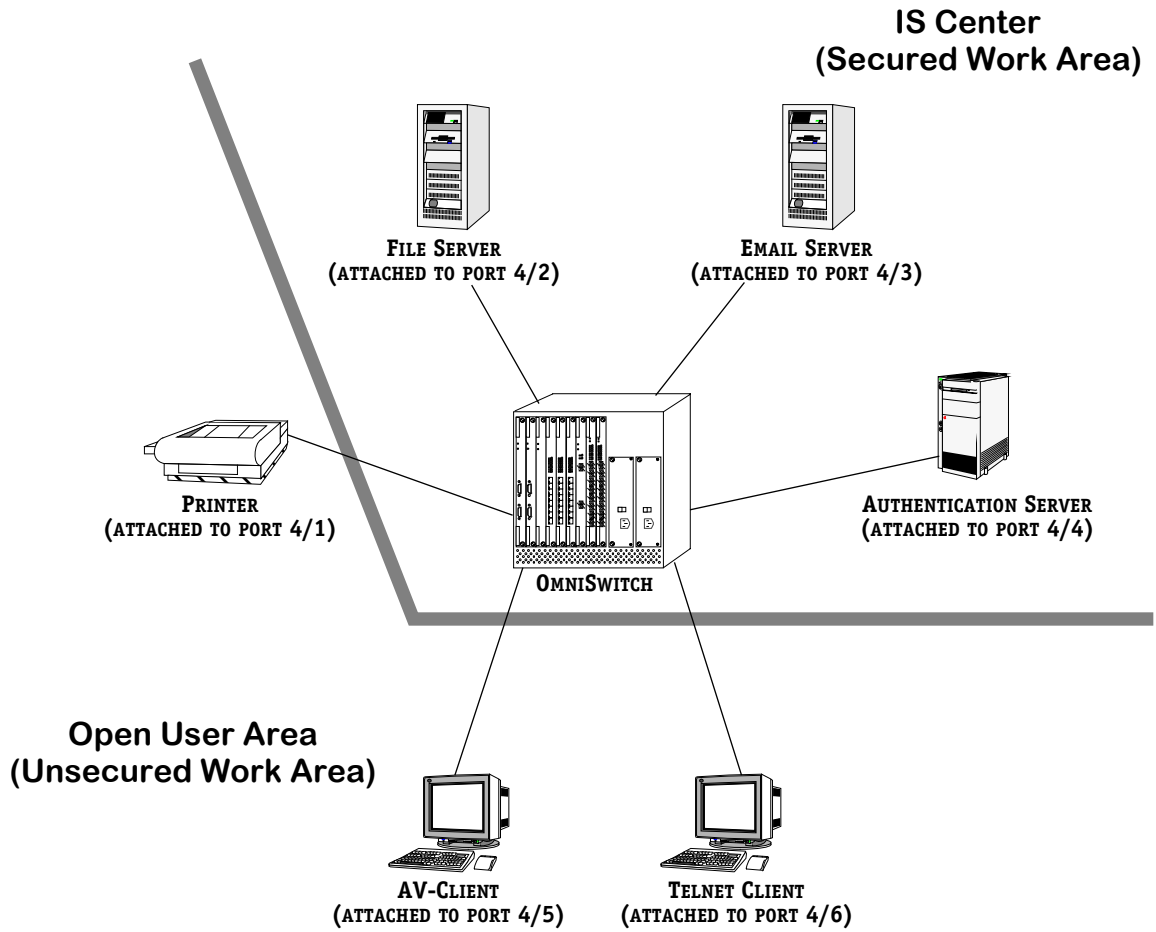
This application example illustrates how the basic components of an authenticated network are configured and how they interact. It includes physically secured devices in an IS Center as well as unsecured user workstations and a printer in main work areas.

It is helpful to look at an authenticated network from a physical and a logical view. The physical view shows the difference between secured and unsecured areas. The logical, or group view, shows how group membership determines user access to network resources.

Physical View

In the diagram below, two workstation clients are present outside the secured area of the IS Center. Authentication controls access to network resources, such as the printer and servers, through a login procedure. Both client stations must log in to gain access to these resources. One of the clients is authenticated through a Windows-based login procedure (the AV-Client), and the other authenticates through a Telnet connection.

The file and email servers are safely behind closed doors in the IS Center. However, user access to these resources through the network will further be guarded by a login procedure. Another network resource, the printer, resides in a physically unsecure area, but the port to which the printer is attached is secured by port binding rules. Seeing how these physical devices are organized into groups will shed light on how user access to devices is controlled.

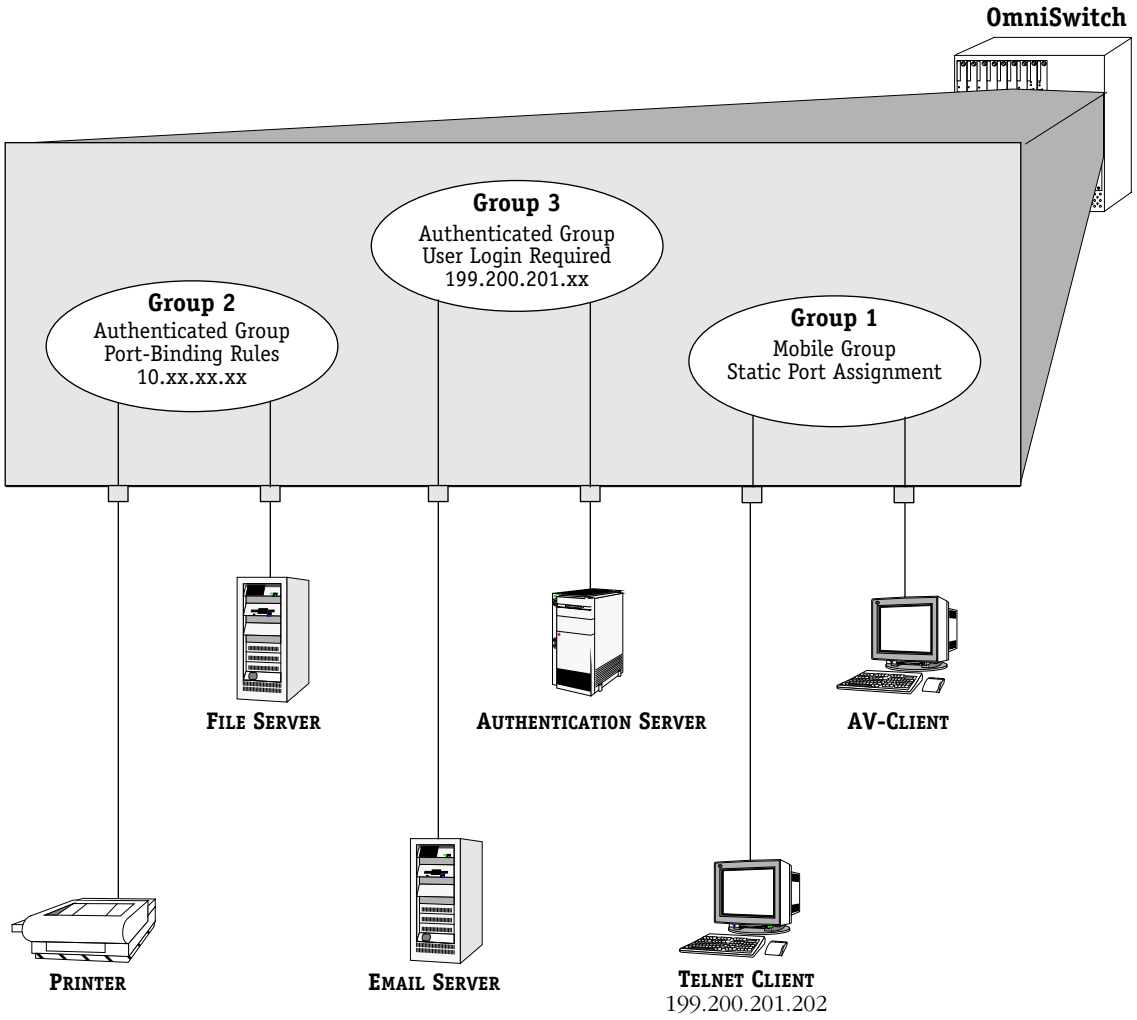


A Physical View of the Network

Logical Group View

The illustration below shows the initial group membership of network devices. The two user devices are first assigned to group 1 since they are attached to ports statically assigned to group 1. In order for either one of them to enroll in group 2 or 3, they must successfully log into those groups (a separate login is required for each group).

The Telnet client will be able to authenticate into group 3 because its IP address belongs to the same IP network as the router port for group 3. The AV-Client could reach either group 2 or group 3 as long as a valid authentication attempt into group 2 or 3 is completed.



A Group View of the Network

The printer device becomes a member of group 2 through a port-binding policy. A port-binding policy is appropriate for this device as it resides in an unsecured area. Another device will not be able to use the printer's network port because it will not be able to easily match all the parameters of the port-binding policy.

The server devices are physically secured in the IS Center, so a port-binding policy is not necessary for these devices. Without the port-binding policies, these devices can be moved around the IS Center with greater flexibility. However, the switch ports to which they connect must be assigned to the groups in which they are members.

How to Set Up this Network

The application example described on the previous pages is configured through the following steps:

Step 1. Configure the Groups

a. Set up group mobility globally for the switch using the **gmcfg** command.

b. Use group 1 as the default client group. By default group 1 will already exist on the switch. Group 1 automatically becomes a mobile group when group mobility is enabled globally on the switch. (The default client group must be a mobile group.) Disable IP routing on group 1 using the **crgp** command. Add the two client ports (4/5 and 4/6) to group 1 using the **addvp** command. These commands are described in the "Managing Groups and Ports" chapter of your switch user manual.

c. Create group 2 as an authenticated group using the **crgp** command. During the **crgp** procedure add the File Server port (4/2) to the group. Also use a port-binding policy to bind the printer to group 2; since the printer is in an unsecured area, the port binding policy ensures that another device with a different MAC address does not take over access to the network through this port.

Also during the **crgp** procedure, configure the protocol for the authenticated group, either IP or All Protocols. If you wanted to use Telnet authentication to access the 10.x.x.x network, enable IP routing and create an IP virtual router port on this group.

d. Create group 3 as an authenticated group using the **crgp** command. During the **crgp** procedure, configure a protocol for the group, either IP or All Protocols, and add the Email Server port (4/3) to the group. Also, enable IP routing and create an IP virtual router port on this group (199.200.201.xx).

Step 2. Configure the Clients

a. Set up the client port (4/6) to be an authenticated port through the **avlPorts** command (see *Configuring Authenticated Ports* on page 1-18. This client station must have its IP protocol stack configured with a network address of 199.200.201.xx. The Telnet client will use group 3's default authentication address (199.200.201.253)—which is created automatically when the authenticated group is created—to authenticate into the group. (If you want to use a different address to authenticate, use the **avladdress** command. See *Setting Up Telnet Clients* on page 1-27 for more information about the **avladdress** command.)

b. Install AV-Client software on the client device, and set up the client port (4/5) to be an authenticated port through the **avlPorts** command. See *Loading AV-Client Software* on page 1-21 for installation information and *Configuring Authenticated Ports* on page 1-18 for information about the **avlPorts** command.

Step 3. Configure the Switch and the Server

a. Enable authentication on the switch. See *Configuring AMC Authentication* on page 1-33, Chapter 2, "RADIUS Authentication," or Chapter 3, "LDAP Authentication."

b. For Check Point authentication, configure user profiles on the AMC through the Windows-based configuration software. You will need to configure authentication type and group membership in the authentication server software. See the *VLAN Authentication Manager-1 Administrator Guide* for more information about configuring the AMC.

c. For RADIUS authentication, see the server manufacturer's documentation for configuration information. For information about server attributes, see Chapter 2, "RADIUS Authentication."

d. For LDAP authentication, see the server manufacturer's documentation and Chapter 3, "LDAP Authentication."

Configuring Authenticated Groups

At least one authenticated group must be configured by creating a new group or modifying an existing group. The group must have group mobility and authentication enabled. A protocol must also be specified for the group.

♦ Note ♦

Group mobility must also be enabled globally on the switch using the **gmcfg** command.

Creating an Authenticated Group

To create a new authentication group, use the **crgp** command. Make sure group mobility and authentication are enabled for the group. During the **crgp** procedure, a prompt displays for enabling group mobility:

```
Enable Group Mobility on this Group ? [y/n] (n):
```

Enter **y** to enable group mobility for the group. The following prompt displays:

```
Enable User Authentication for this Group ? [y/n] (n):
```

Enter **y** to enable authentication for the group. A prompt will display for configuring a protocol for the group. See the next section, *Specifying a Protocol* on page 1-12, for information about configuring the protocol. Additional prompts display during the **crgp** procedure for adding switch ports to the group, adding auto-activated LANE services, and configure AutoTracker port-binding policies for the group. See the "Managing Groups and Ports" chapter of your switch manual for more information about this command.

Modifying an Existing Group for Authentication

To configure an existing non-authenticated group for authentication, use the **gmstat** command to enable group mobility for the group and the **mag** command to enable authentication on the group. See the "Managing Groups and Ports" chapter of your switch manual for information about the **gmstat** command, and *Modifying an Authenticated Group* on page 1-13 for information about the **mag** command.

Specifying a Protocol

During the **crgp** procedure or the **mag** procedure, you will be asked to select a protocol for the authenticated group. Since authenticated groups do not support protocol or network address policies, there is no way to tell the protocol of such a group by its policies. Therefore, the following prompt allows you to clearly specify the protocol supported by the authenticated group:

```
Select Protocol for this group:
1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type (in hex)
6. Protocol specified by DSAP and SSAP
7. Protocol specified by SNAP
8. ALL PROTOCOLS
```

Options for specialized protocols configured with ether-type, DSAP/SSAP, and SNAP information are described in the "AutoTracker Policies" chapter of your switch manual. Documentation for the full **crgp** procedure can be found in the "Managing Groups and Ports" chapter of your switch manual. The **mag** command is described in this chapter in *Modifying an Authenticated Group* on page 1-13.

Viewing Current Authenticated Groups

Use the **vag** command to view the currently configured authenticated groups. If you enter **vag**, a screen similar to the following displays:

```
Group ID    Protocol
==================
   6          Protocol = IP
```

Group ID. The authenticated group number.

Protocol. This column describes the protocol supported by this group as specified during the **crgp** or **mag** procedure.

Modifying an Authenticated Group

Use the **mag** command to enable or disable authentication on a mobile group, configure an authenticated group's protocol, and configure binding policies. (Use the **gmstat** command to enable mobility on an existing group.) Follow these steps to modify a mobile group's authentication parameters:

1. Enter **mag** at the system prompt.
2. The following prompt displays:

   Enter the Authenticated Group Id to modify:

   Enter the group number that you want to modify. The **mag** command only operates on mobile groups. You can modify an existing authenticated group or enable authentication on an existing mobile group. If you enter a group number for a non-mobile group here, then the following prompt displays:

   Group X is not a mobile group. Please try again.

3. If you enter a mobile group number, a prompt similar to the following displays:

   Authentication is Enabled for Group X. Disable Authentication ? [yes/no] (no) :

   This prompt displays the status of authentication for the mobile group. In this example, if you want to enable authentication, simply press **<Enter>**. If you choose to disable authentication, then you will exit the **mag** command.

4. If authentication is enabled, the following prompt displays:

   Configure the Protocol for this Authenticated Group ? [yes/no] (yes) :

   Select whether or not you want to configure the protocol used in this authenticated group. If you select **Yes** at this prompt, then the protocol selection menu displays:

   Select Protocol for this group:
   1. IP
   2. IPX
   3. DECNET
   4. APPLETALK
   5. Protocol specified by ether-type (in hex)
   6. Protocol specified by DSAP and SSAP
   7. Protocol specified by SNAP
   8. ALL PROTOCOLS
   Enter protocol type (1) :

   Enter the line number for the protocol you want this authenticated group to support. Options for specialized protocols configured with ether-type, DSAP/SSAP, and SNAP information are described in the "AutoTracker Policies" chapter of your switch manual.

5. The following prompt displays:

   Configure binding policies for this Authenticated Group ? [yes/no] (yes) :

   Indicate whether you want to configure binding policies on this authenticated group. The procedure for configuring binding policies is fully described in the "AutoTracker Policies" chapter of your switch manual.

   When you have completed setting up binding rules, the **mag** command indicates the group was modified and the system prompt displays.

   ♦ Note ♦

   If you want to add more binding rules later, use the **modavtl** command.

User Authentication UI Commands

Use the user authentication commands to configure the agent's (switch's) interface to the client and the server. For general information about the User Interface (UI), see your switch user manual.

♦ Note ♦

The commands are not case sensitive. They are shown in upper and lowercase for ease of reading.

There are several commands for configuring parameters that relate to the authentication client. A login banner may be created for either AV-Client or Telnet clients (see *Creating the Authentication Client Banner* on page 1-17). Telnet addresses and ports may be configured as described in *Setting Up Telnet Clients* on page 1-27.

If you are using Check Point (AMC) Authentication, you must enable authentication on the switch and configure the IP address and other parameters of the AMC through the **fwconfig** command. See *Configuring AMC Authentication* on page 1-33 for more information on the **fwconfig** command. (The **fwd.img**, **fw4.img**, or **fwx.img** image file must be loaded in the switch.)

If you are using Layer 2 Authentication (RADIUS or LDAP), you must enable authentication on the switch using the **layer2auth** command. (The **rav.img** image must be loaded in the switch.) You must also configure the mode and add RADIUS or LDAP servers to the configuration. Additional commands for these tasks are listed in Chapter 2, "RADIUS Authentication," and Chapter 3, "LDAP Authentication."

Security Menu Commands

A user authentication submenu is available from the Security menu when authentication is enabled using the **fwconfig** command or the **layer2auth** command:

Command	Security Menu
pw	Set a new password for a login account
reboot	Reboot this system (allowed if the user has WRITE privilege)
timeout	Configure Auto Logout Time
layer2auth	Enable/Disable Layer2 user authentication
secuser	Configure Secure Access user definitions
secproto	Configure Secure Access IP protocols
seclog	Show Secure Access entries in the mpm.log file
UserAuth	Enter the Layer 2 User authentication menu

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

For information about the **pw**, **reboot**, **timeout**, **secuser**, **secproto**, and **seclog** commands, see the Switch Security chapter in your switch manual.

The User Authentication submenu display depends on which type of authentication is enabled. If AMC 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 an Authenticated port
avlsPorts	Show ports that are Authenticated ports
avlWebPath	Set a path restriction on Authentication web pages
avlsWebPath	Show the path restriction on Authentication web pages

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

Managing Authentication Clients

If you are using a login procedure to authenticate user devices in the network, then you will need to configure parameters for authentication clients. There are two types of clients that may reside in your network: AV-Client clients and Telnet clients. (Note that the AV-Client is not supported over Token Ring.)

AV-Clients require the installation of the Microsoft DLC protocol and the AV-Client software. AV-Client configuration is covered in *Installing AV-Clients* on page 1-19.

Telnet clients do not require any special software on user devices other than a standard Telnet client application, but you still must configure authentication ports and router addresses on the switch. Telnet client configuration is covered in *Setting Up Telnet Clients* on page 1-27.

Authentication may have a slight impact on switch performance during user login and logout procedures (i.e., performance may be affected at the beginning and end of the work day). The maximum number of users that can be in the process of logging in simultaneously is 100.

Both AV-Client and Telnet client stations display a banner during the login process. The steps for configuring and viewing that banner are described here.

Creating the Authentication Client Banner

When a user attempts to log in to an authenticated group, a banner will be displayed during the log-in procedure for both the AV-Client and the Telnet client. You define this banner through the **avlbanner** command. Follow these steps:

1. Enter **avlbanner** at a switch system prompt. The following prompt displays:

   ```
   Enter Client Authentication banner ():
   ```

2. Enter the authentication client banner that you want to display at users' workstations. You may specify up to 40 characters per line. To specify multiple banner lines, end each line that is not the final line with a backslash character followed by the letter "n" (**\n**); you will be prompted for the next line. You can specify up to 512 characters for the entire banner.

   Press **<Enter>** when you are done entering the final line of the banner.

3. The banner you entered is displayed for your confirmation:

   ```
   The banner looks like:
   Welcome to the Group Authentication Process
   Do you wish to re-enter the banner (No) :
   ```

4. Indicate whether or not you want to re-enter the banner. If you do not need to change it, then simply press **<Enter>**. If you choose to re-enter the banner, enter **Yes** and repeat Steps 1 through 4.

Viewing the Current Authentication Client Banner

Using the **avlsbanner** command, you can view the authentication client banner previously entered through the **avlbanner** command. To view the current authentication client banner, enter **avlsbanner** at a switch system prompt. A screen similar to the following displays:

```
The Client Authentication Banner is:
Welcome to the Group Authentication Process
```

The second line displays the actual banner. You can always change this banner through the **avlbanner** command.

Configuring Authenticated Ports

All physical ports that will be used for authentication must be configured using the **avlPorts** command. Follow the steps here:

1. At the system prompt, enter the **avlPorts** command. The following prompt displays:

   ```
   Do you wish to add or delete a port (add) :
   ```

2. If you want to add a port to the supported authentication ports list, then enter an **a**. If you want to delete a port from the supported ports list, then enter a **d**.

3. The following prompt displays if you chose to add ports:

   ```
   Which ports do you wish to add:
   ```

   The following prompt displays if you chose to delete ports:

   ```
   Which ports do you wish to delete:
   ```

   Enter the list of ports that you want to add or delete. First enter the module's slot number, followed by a slash (/), and then the port number of the module. For example, port 2 on the module in slot 4 would be entered as **4/2**. You can enter multiple (and ranges of) ports. Press **<Enter>** when you are done entering ports.

4. A list of the ports you entered displays. The following is a sample display of an added port:

   ```
   Port 4 set to Auth Vlan Port
   ```

   The following is a sample display of a deleted port:

   ```
   Port 4 returns to normal port
   ```

Viewing Current Authenticated Ports

Using the **avlsPorts** command, you can view the switch ports that have been configured to support authentication connections. These ports are specified through the **avlPorts** command. To view this list, enter **avlsPorts**. A screen similar to the following displays:

```
Current Authentication Ports
 Slot / Port
   2 / 4    2 / 6
```

You can add or delete ports from this list through the **avlPorts** command.

Installing AV-Clients

The Alcatel Authenticated VLANs Client (AV-Client) is Windows-based software that may be used for authentication. AV-Clients rely on the DLC protocol (rather than IP) to communicate with the authentication agent in the switch. Because the AV-Client does not require an IP address and can move into any authenticated group without one, the AV-Client is recommended in networks where there are multiple authenticated groups.

♦ Note ♦

The AV-Client is not supported over Token Ring.

In addition to installing the client software, you must configure the switch so that it knows the physical ports through which AV-Clients will authenticate. You configure these ports through the **avlPorts** command described in *Configuring Authenticated Ports* on page 1-18.

The AV-Client software requires two main installation steps:

Step 1. Load the Microsoft DLC Protocol Stack

The AV-Client login procedure requires the Microsoft DLC protocol. You need to install the protocol. The procedures for loading on Windows 95, Windows 98, and Windows NT stations are described in *Loading the Microsoft DLC Protocol Stack* on page 1-19.

Step 2. Load the AV-Client Software

The AV-Client authentication software must be loaded on all Windows-based devices you want to authenticate. This Wizard-guided installation procedure is described in *Loading AV-Client Software* on page 1-21. The procedure installs the AV-Client on the Windows desktop and also installs an AV-Client configuration utility in the Windows Control Panel.

Loading the Microsoft DLC Protocol Stack

Windows 95 Stations

You need to install the DLC protocol program and the DLC protocol program update patch from the Microsoft FTP site (ftp.microsoft.com). Once connected to the FTP site, go to the Softlib/Mslfiles directory and retrieve the MSDLC32.EXE file. Also download the DLC32UPD.EXE file (or the latest DLC protocol update). These files are self-extracting zip files. Follow these steps to load these files on a user station:

a. Double-click the MSDLC32.EXE file in the folder to which you want to download the file.

♦ Note ♦

Do not run MSDLC32.EXE file in the Windows or Windows\System folders. If you downloaded the file to either of these locations, copy it to a temporary folder on your hard disk or copy it to an installation diskette before double-clicking on it.

b. Click on the Start button, highlight the Settings menu, and then click on Control Panel.

c. Double-click the **Network** icon in the Control Panel.

d. In the Network dialog box, click on the **Add...** button.

e. In the Select Network Component Type dialog box, double-click on the **Protocol** network component.

f. In the Select Network Protocol dialog box, click on the **Have Disk...** button.

g. Specify the drive and path where the MSDLC32.EXE files (you should have already extracted them) are located. For example, if you created an installation diskette, you would enter:

<drive letter>:

If you created a temporary folder on your hard disk, then you would enter:

c:\<folder name>

where <folder name> is the directory into which you copied the MSDLC32.EXE files.

h. Click OK.

i. Click "Microsoft 32-bit DLC" and then click OK.

j. When prompted, insert the Windows 95 disks so that other network components can be reinstalled.

k. When prompted, shut down your computer and restart Windows 95. This restart is required for the DLC protocol stack to load on the system.

l. Next the DLC protocol stack update must be loaded. Double click the DLC32UPD.EXE file. The program will install itself. After installing the update, it is recommended that the system be rebooted.

Windows 98 and Windows NT Stations

The installation of the DLC protocol stack requires files from the Windows 98 or Windows NT distribution software. Make sure you have your Windows 98 or NT media available during this procedure. Follow these steps:

a. Select the Control Panel for Network.

b. Select the Protocols tab.

c. Click Add.

d. Select the DLC Protocol.

e. Click OK.

f. Follow the prompts requesting Windows 98 or NT files.

Loading AV-Client Software

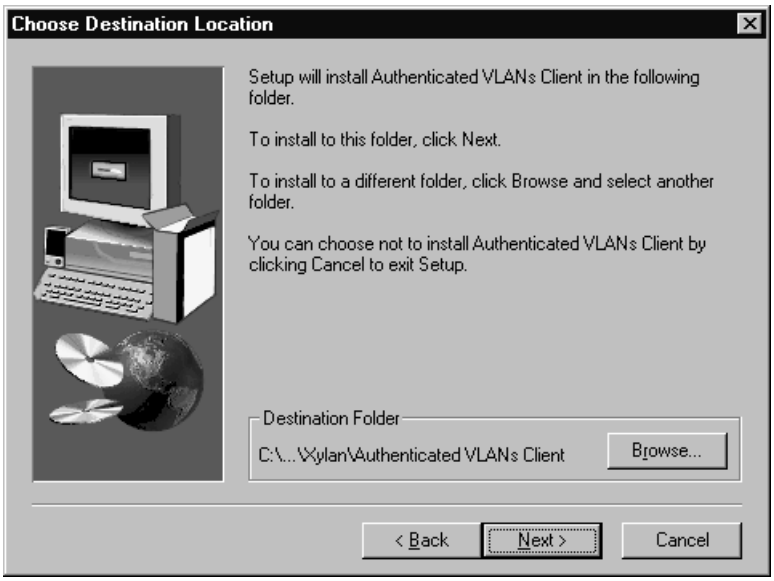
The following procedure installs the AV-Client on the Windows desktop and an AV-Client configuration utility in the Windows Control Panel.

a. Insert the disk with AV-Client software into your A: drive.

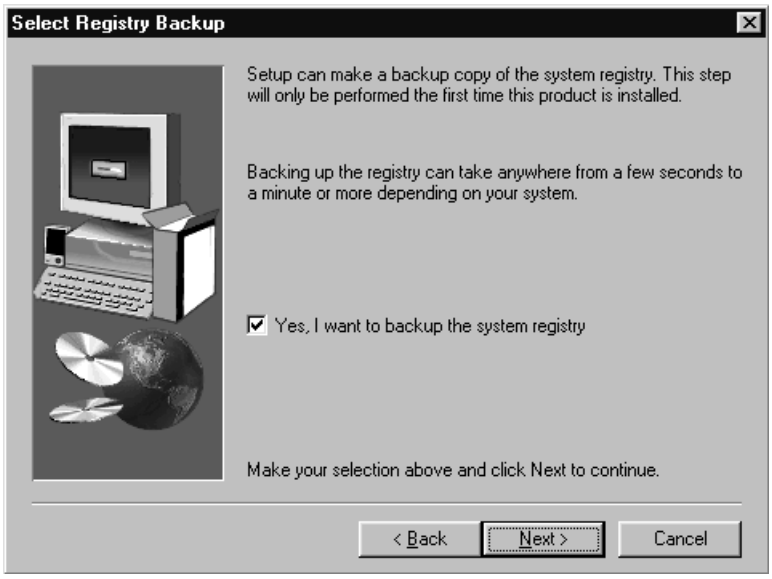
b. Select the **Run** option from the Start menu.

c. Enter **a:setup.exe** in the Run field. The authentication client installation procedure begins, and the following window displays:

d. Click on the **Next...** button. The following window displays.

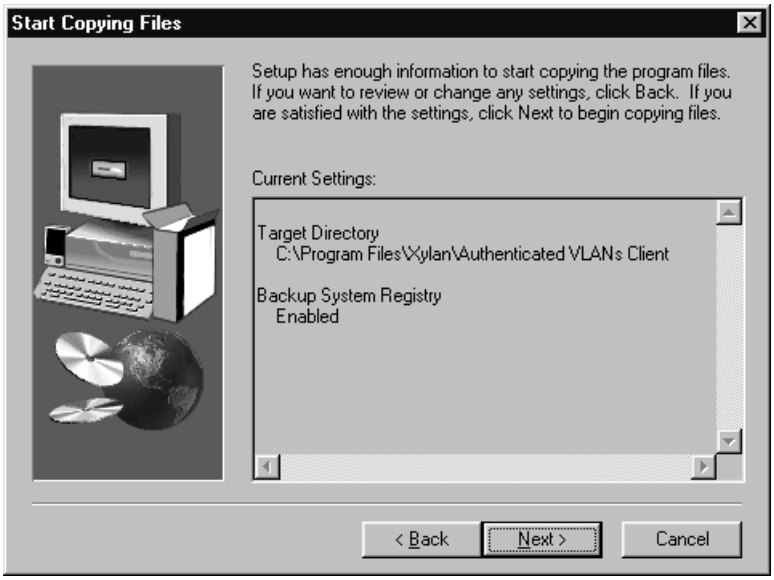


e. Click on the **Next...** button. The following window displays for backing up the Windows system registry. The registry is backed up by default. If you do not want to back up the system registry, click the box to deselect the backup option. Typically this option should be selected.



f. Click on the **Next...** button. If the registry backup option is enabled, the following window displays. (If you deselected the backup option, go to step h.)

g. Click on the **Next...** button. The following window displays.



h. Click on the **Next...** button. A status bar displays indicating what percentage of the software is loaded. When it is finished loading, the client authentication screen displays with the authentication banner. You can start an authentication session (see *Logging Into the Network Through an AV-Client* on page 1-26) or close the window. If you close the window, or when you exit the authentication session, the following window displays.

You can run the AV-Client without rebooting, but the configuration utility will not be available until you reboot the system.

Using the AV-Client Configuration Utility

The AV-Client includes a utility for configuring whether or not the client is enabled at system startup. To run the utility, install the AV-Client and reboot the system. By default, the AV-Client is enabled, and the client login window displays at system startup. The configuration utility also allows you to enable/disable DHCP renew/release for authentication login/logoff or configure the delay between sending a DHCP release packet to the DHCP server and a logoff packet to the switch. By default DHCP renew/release is enabled, and the default delay for release/logoff is 2 seconds.

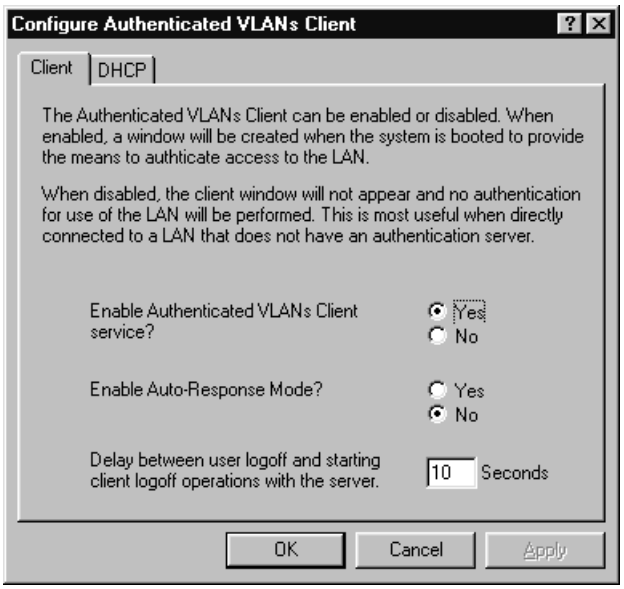
A delay between DHCP release and client logoff is recommended because the DHCP server's MAC address may be timed out in the AV-Client's ARP table. If that is the case, the client must send an ARP packet to discover the DHCP server's MAC address before it can send the release packet. If the logoff packet is sent to the switch before the release packet gets sent, then the IP address will never be released. Increasing the value of the delay parameter can prevent this from happening.

The following sections explain how to use the configuration utility.

Enabling/disabling the AV-Client at Startup

To enable/disable the AV-Client at startup:

1. Double-click on the Authenticated VLANs Client icon in the Control Panel, and the following screen displays:



2. Click on Yes or No to enable or disable authentication at the next startup.

3. Click on Yes or No to enable or disable auto-response mode. When this mode is enabled, the client "remembers" the user ID and password. After initial logon, whenever the client is restarted, the user ID and password do not have to be entered.

♦ Important Note ♦

The auto-response mode is disabled by default and should only be enabled on a secure, single-user system.

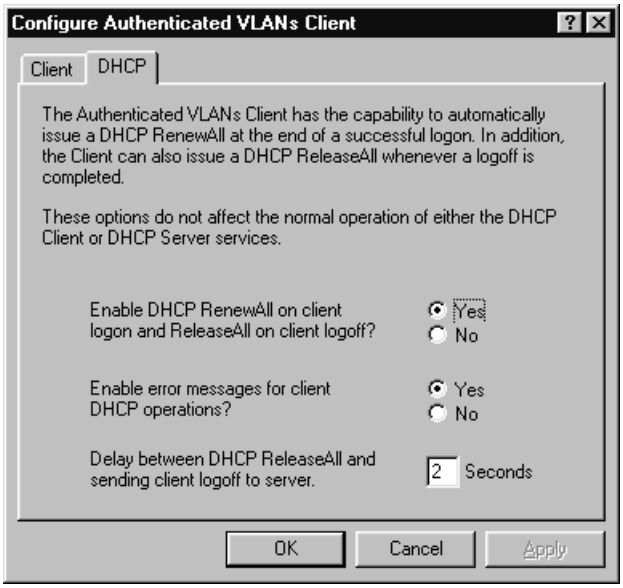
4. The default delay between the client initiating a logoff and the actual disconnection from the server is 10 seconds. Increase or decrease the delay if required by entering the desired value.

5. Click OK to save the changes.

Configuring AV-Client DHCP Parameters

To configure DHCP renew/release, enable DHCP errors, or configure the delay between renew and logoff, following the steps here:

1. Click on the DHCP tab, and the following screen displays:



2. Click on Yes or No to enable or disable DHCP renew/release. *If you are using DHCP to get an IP address, this option should always be enabled. If you are not using DHCP, the setting for this option has no effect.* (An IP address is not required for the AV-Client to authenticate.)

♦ Note ♦

If you disable the renew/release option, an IP address will not be automatically assigned to your user station when you authenticate using the AV-Client. If you want to use IP in this scenario, you will have to manually execute a DHCP renew process through some other Windows utility.

3. Click on Yes or No to enable or disable DHCP error messages.

4. To configure a different delay, enter the desired number of seconds.

5. Click on OK to save the changes. Any changes you make will take effect immediately. A reboot is not required.

Logging Into the Network Through an AV-Client

Once the AV-Client software has been loaded on a user's PC, an AV-Client icon will be created on the Windows desktop in the task bar. Follow these steps to log into the authenticated network:

1. Double-click the icon to start the login procedure. A window will display with the following messages:

   Welcome to the Xylan Client Authentication System

   User:

   The banner configured with the **avlbanner** command displays first. The User ID prompt is displayed by the authentication server.

2. Enter the user name for this device. This user name is configured on the authentication server.

3. The following prompt displays:

   <Password Type> password:

   Enter the password for this user. If the user enters the correct password, then the following message displays:

   User xxxxx authenticated by <Authentication Type> authentication

   The user is now logged into the network and has access to all network resources in the group with which this user shares membership.

♦ Note ♦

If authentication is successful but an error was made while configuring groups, the user station may not move into the group the user requested.

Setting Up Telnet Clients

Telnet clients authenticate through a Telnet session. No specialized authentication client software is required on Telnet client stations. However, you do need to configure the switch so that it knows the physical ports through which Telnet clients will authenticate. You configure these ports through the **avlPorts** command.

You may also need to configure the address of the router through which Telnet clients must communicate to reach the authentication server. This authentication IP address is entered through the **avlAddresses** command. The Telnet authentication IP address does not need to be unique among a group of switches using authentication; this address is only visible on ports that have been configured to accept Telnet authentication requests.

If you will be using DHCP to get an IP address for the Telnet client, you may need to configure a BOOTP relay as described in *BOOTP Relay for Telnet Authentication* on page 1-32.

The following sections describe how to configure and view Telnet client parameters.

Defining Telnet Authentication Addresses

The **avlAddresses** command allows you to configure the IP address of the service through which Telnet users are authenticated. To define these addresses, follow these steps:

1. Enter **avlad** (this is the shortest usable form of the **avlAddresses** command). The following prompt displays

   Router interface address: () :

2. Enter the IP address of a router interface that is on the same network/subnetwork as the Telnet access address that you wish to configure. The following prompt displays:

   Authentication address: () :

3. If you have devices using Telnet to authenticate, then you need to enter the IP address of the Telnet authentication service that the Telnet clients will use to initiate a Telnet authentication session.

Viewing Current Telnet Authentication Addresses

The **avlsaddresses** command displays all authentication port addresses configured through the **avladdresses** command. When you enter **avlsa**, a screen similar to the following displays:

Group : Vlan	IP address	Authentication IP address
1:0	192.168.10.1	192.168.10.253
7:0	200.2.2.100	200.2.2.253
2:0	198.206.184.100	198.206.184.253

Group:Vlan. The group and VLAN for which these authentication addresses are configured. Since authenticated groups must be mobile groups, the VLAN value will always be zero (since no VLANs can be configured on mobile groups).

IP address. The IP address of a router port on the switch.

Authentication IP address. The IP address of the Telnet authentication service.

Configuring an Authentication Host Name

If the Telnet client is configured to use a web browser, you may want to configure a host name to correspond to the Telnet address (x.x.x.253). When clients attempt to authenticate, they can enter the host name rather than type the IP address in the browser command line.

To configure an authentication host name, follow the steps here:

1. At the system prompt, enter the **avldnsname** command. A screen similar to the following displays:

   ```
   The authentication host name is not configured.
   Do you wish to change the authentication host name,
   disable authentication DNS or exit (c, d or e)? (exit):
   ```

2. Type **c** to configure the host name. The following prompt displays:

   ```
   Enter the host name used for authentication ():
   ```

3. Enter the relevant host name.

Disabling an Authentication Host Name

Once a host name is configured it may be disabled using the **avldnsname** command. To disable the DNS host name, follow the steps here:

1. At the system prompt, enter the **avldnsname** command. A screen similar to the following displays:

   ```
   The authentication host name is not configured.
   Do you wish to change the authentication host name,
   disable authentication DNS or exit (c, d or e)? (exit):
   ```

2. Type **d** to disable the DNS host name.

To re-enable the host name, you must use the **avldnsname** command and specify the host name again.

Viewing the Current Authentication Host Name

To display the current host name, use the **avlsdnsname** command. A message similar to the following displays:

```
The configured authentication host name is “wolfie”.
```

You can change the host name through the **avldnsname** command.

Setting a Web Path Restriction

If the Telnet client is configured to use a web browser, you may want to configure a web path restriction to limit the web pages on the switch that are available to authenticated users. The configured path must match the path configured for authentication in the switch's internal web server. *Note that the switch's internal web server will be available in a future release.*

To configure a web path restriction, enter the following command:

```
avlWebPath
```

A message similar to the following displays:

```
Enter the Web Path restriction for Authentication () :
```

Enter the relevant path for authenticated users. For example:

```
authentication
```

Only pages located along the **/authentication** path will be accessible to the user.

Viewing a Web Path Restriction

To view a web path restriction, enter the following command:

```
avlsWebPath
```

A message similar to the following displays:

```
The Web path restriction is: authentication
```

Logging Into the Network Through a Telnet Client

Once you have correctly configured your Telnet switch and router ports, your client devices may log into the network. This section describes the log-in procedure for a PC user.

1. Using standard Telnet software, start a new Telnet session by connecting to port 259. An example of a Telnet command line would be:

   telnet 192.168.10.253 259

   where **telnet** is the command, **192.168.10.253** is the telnet authentication IP address (configured through the **avladdresses** command), and **259** is the special authentication port. See your Telnet software documentation for specific information about the format of this command.

2. The following screen displays:

   Welcome to the Xylan Client Authentication System

   Action: [1] Logon [2] Logoff:

   Enter a **1** at this prompt and press **<Enter>**.

3. The following prompt displays:

   User:

   Enter the user name for this device. This user name is configured on the authentication server.

4. The following prompt displays:

   <Password Type> password:

   Enter the password for this user. If the user enters the correct password, then the following message displays:

   User xxxxx authenticated by <Authentication Type> authentication

   The End

   Once authenticated, the Telnet session ends, and the user device can access all network resources in groups in which it is a member.

♦ Note ♦

The previous message means the user authentication was successful. However, if an error was made while configuring groups, the user station may not actually move into the group the user requested.

Authentication Clients and DHCP

DHCP is a convenient way to assign IP addresses to an authentication client. A DHCP server integrated in the switch allows for direct configuration of IP addresses for clients or it may function as a proxy for another DHCP server. The DHCP server may be configured as part of the default client group, an authenticated group, or both. The configuration depends on how your network is set up and determines how the authentication client will receive an IP address.

After booting up, authentication clients are initially part of a default client group on the switch. An AV-Client does not need an IP address to authenticate out of the default group and into an authenticated group (though it may require an IP address for other kinds of communication). But a Telnet client must have an IP address in order to authenticate into an authenticated group.

♦ Note ♦

In general, the DHCP server should *not* be configured for the default client group because it is difficult to manage the server from an authenticated part of the network.

The DHCP server can supply IP addresses for a particular subnet, and that subnet corresponds to one particular authenticated group. Typically a DHCP server is configured to be part of an authenticated group. The authenticated group must be configured for IP (see *Specifying a Protocol* on page 1-12).

Addresses supplied by the DHCP server may have to be configured as "short leases" if authentication clients will be releasing an IP address and getting a new IP address in another group. Note that the Telnet release/renew process is problematic. It requires manual intervention because the Windows DHCP client does not expire IP addresses correctly.

AV-Client and DHCP

For an AV-Client, DHCP configuration is not required. AV-Clients do not require an IP address to authenticate, but they may want an IP address for IP communication in an authenticated group.

At startup, an AV-Client user station will issue a Windows DHCP request if the AV-Client's DHCP release/renew feature is enabled. (The feature is enabled by default. See *Using the AV-Client Configuration Utility* on page 1-24.) The AV-Client is capable of obtaining an address from the default client group or whatever group it authenticates into if a DHCP server is located in the group.

Because the AV-Client does not require an IP address and can move into any authenticated group without one, the AV-Client is recommended in networks where there are multiple authenticated groups.

Telnet Client and DHCP

For a Telnet client, the location of the DHCP server is important because an IP address is required for authentication.

In networks where there is one authenticated group and one DHCP server located in *either* the default client group *or* the authenticated group, the Telnet client will obtain an IP address directly from a server in the default client group, or indirectly via BOOTP relay to a DHCP server in the authenticated group. (BOOTP relay for authentication is described in the next

section.) In either case the DHCP server is configured with IP addresses associated with the authenticated group subnet, and the Telnet client obtains an address that is valid for authenticating into the group.

In networks using multiple authenticated groups, using the Telnet client is not recommended. (The AV-Client is recommended if your network has multiple authenticated groups.) When using a Telnet client with multiple authenticated groups, each authenticated group must have its own DHCP server. The Telnet client must release the IP address it first obtains at startup through the default group and get a new address from a DHCP server located in the group it is authenticating into. The Telnet release/renew process is problematic. It requires manual intervention because the Windows DHCP client does not expire IP addresses correctly.

BOOTP Relay for Telnet Authentication

If a DHCP server is configured for the authenticated group, the startup DHCP request from a Telnet client may be tunnelled from the default client group to the authenticated group via BOOTP relay. BOOTP relay is configured using the **relayc** command. For more information about this command, see the UDP Forwarding chapter of your switch manual.

The router port address of the authentication group must also be configured for the relay. To configure this address, follow the steps here:

1. At the system prompt, enter the **avlbootpmode** command. A prompt similar to the following displays:

   Authentication BOOTP relay is currently disabled.
   Do you wish to enable? (yes) :

2. Press **<Enter>** to change the setting. The following prompt displays:

   Please choose the interface address from the list below:

   1. 192.168.10.1
   2. 198.206.184.178

   Enter the number corresponding to the IP address:

3. Enter the number corresponding to the router port through which the DHCP server may be reached.

Viewing the Current Status of the BOOTP Relay

To display the current status of BOOTP relay mode, use the **avlsbootpmode** command. A message similar to the following displays:

Authentication BOOTP relay is enabled using interface: 172.16.183.20

Configuring AMC Authentication

The Authentication Management Console (AMC) uses Check Point's proprietary authentication protocol. The software running in the switch that supports the AMC Authentication feature is accessed using the **fwconfig** command. This command is also used to configure the IP Firewall feature which is described in Chapter 4, "IP Firewall." Both of these features provide a means of securing your network(s) and switch(es) and both are based on products licensed from Check Point Technologies, Inc.

The switch software accessed by the **fwconfig** command can operate in *either* Authentication mode or in Firewall mode, but *not* in both modes simultaneously. This restriction means that in order to use both the IP Firewall and AMC Authentication software at the same time in a single network you must have at least two switches connected to the network (one switch operating in Firewall mode, the other in Authentication mode). Because the **fwconfig** command is used to serve these two purposes, some of the prompts displayed by the command refer to the Firewall mode (because it is the default) until you have selected the Authentication mode.

There are three steps involved in configuring the firewall/authentication software for the first time. Due to the design of the software, these steps are performed sequentially as follows:

1. Display the current configuration of the firewall/authentication software.
2. Modify the software's configuration by selecting the desired operating mode (in this case, "Authentication") and by specifying the required configuration parameters. When configuration is completed, the software will begin operating in the selected mode.

In general, you will need to configure the authentication software only once. After you have completed the initial configuration, you will only need to make adjustments if you: 1) need to reset an Skey password, or 2) need to change the IP addresses of an AMC, or 3) need to change this switch to operate in the Firewall mode. If you *do* find in the future that you need to make changes to the IP address of an AMC, simply follow the configuration steps under Step 2 (below) again to make the change. You will have to reboot the switch to implement the change of IP address.

Step 1. Displaying the Current AMC Configuration

Follow the steps below to display the current configuration of the software.

♦ Note ♦

If Layer 2 Authentication (RADIUS or LDAP) is enabled, AMC Authentication cannot be configured. Disable Layer 2 Authentication using the **layer2auth** command and reboot the switch. For more information about the **layer2auth** command, see *Security Menu Commands* on page 1-15 as well as Chapter 2, "RADIUS Authentication" and Chapter 3, "LDAP Authentication."

a. At the system prompt, enter the **fwconfig** command. (This command can be abbreviated to **fwc**.) The following prompt displays:

```
View existing configuration? (y or n) (y) :
```

b. Enter **y** (or just press **<Enter>)** to display the existing configuration.

Because the software is disabled at this point, a screen similar to the following displays:

```
Firewall is Disabled

Primary manager IP address = none

Secondary manager IP address = none

Time zone offset to UTC = 0 hours

Default switch interface mode = Open

Modify existing configuration? (y or n) (n) :
```

Because the software in this switch has never been configured before, the display shows that the Firewall is currently disabled (because this is the default mode) and that none of its parameters have been set. These parameters are explained fully in the steps below.

Step 2. Modifying the AMC Configuration

a. The above prompt asks if you want to modify the existing configuration:

```
Modify existing configuration? (y or n) (n) :
```

Enter **y** to change the configuration.

b. The following prompt displays:

```
Change firewall state to Enable? (y or n) (n) :
```

Enter **y** to enable the software. Keep in mind the software will *not* start operating until you have reached the end of the configuration steps.

c. The following prompt displays:

```
Enable:
  Firewall ------- f
  Authentication - a ? (f) :
```

This prompt asks if you want the software in the switch to operate in the Firewall mode or Authentication mode. Remember, you can choose only *one* of these two modes at any given time. To switch between these two modes, you must first disable the software, reboot the switch, then re-enable the software in the desired operating mode.

Enter **a** to select the Authentication mode.

d. The following prompt displays:

```
Change primary management station address? (y or n) (n) :
```

Enter **y** to change the IP address of the workstation to be used as your primary AMC.

e. The following prompt displays:

```
Enter primary management station IP address :
```

Enter the IP address of an existing AMC already configured for use with this switch (this was done when you configured the switch as one of the AMC's "remote modules").

f. The following prompt displays:

```
Reinitialize primary's skey password? (y or n) (n) :
```

Enter **y** to proceed to enter the Skey password needed to connect to the AMC. Because this is your first-time configuration, you must answer "Yes" to this prompt.

g. The following prompt displays:

```
Enter skey password :
```

Enter the password that was previously specified for use with this switch (you entered a password for this switch when you configured the AMC's "remote modules"). Unless you enter the *exact* password here that the AMC *already* knows about, you will not be able to establish a communications link with the AMC.

Important Notes about Passwords

The password is automatically changed according to Skey algorithms after a selected number of transactions have occurred between the switch and the AMC. Therefore, the current password *cannot* be displayed on the switch as it is continually being changed over time according to the Skey rules. The switch and the AMC both maintain a copy of the password (in their respective configuration files), which is preserved between reboots. In most cases, you will have to enter the password only one time. However, if you should delete the switch's configuration file (the file is named **mpm.cnf**), you will have to re-enter a password on *both* the AMC and the switch.

h. The following prompt displays:

```
Offset in hours from Universal Time (UTC or GMT; i.e, PST= -8, PDT = -7)
    (Hit <enter> to keep current value) :
```

The "time zone offset" specifies the number of hours that must be added to, or subtracted from, *your* local time zone in order to match Universal Time Coordinates (UTC), also known as Greenwich Mean Time (GMT). The switch uses this parameter to enter the correct timestamp on events, logs, and alert messages sent to the AMC. The range is plus 10 hours to minus 13 hours. The major time zones in the United States are all "*negative*" values: -8 (Pacific), -7 (Mountain), -6 (Central), and -5 (Eastern). You will need to set this parameter only if you want to normalize message logging on the AMC to UTC.

Enter a whole number in the range (plus) 10 to (minus) -13, for example, **-8**.

i. A message similar to the following displays:

```
Firewall configuration change successful.

fwdSpawn done! fwdTaskId = 0x48BDE620

vauthdSpawn done! vauthdTaskID = 0x48BC3710
```

The system prompt will then redisplay, and AMC authentication will immediately become active.

j. To check the configuration parameters you have just made, you can re-enter **fwconfig**.

A screen similar to the following displays:

```
Authentication is Enabled
    for Vlan Authentication only function

Running Xylan Authentication Version 3.2.1.31

Primary manager IP address = 198.206.184.58
    The state of the connection to this manager is : CONNECTED

Time zone offset to UTC = -8 hours

Modify existing configuration? (y or n) (n) :
```

This screen shows that the software is currently enabled in the "Authentication" mode. Also indicated are the version number of the installed software, the IP address of the AMC, the state of the connection to the AMC, and the specified time zone offset of this switch from Universal Time Coordinates (UTC).

Disabling AMC Authentication

Follow these steps to disable the authentication software in the switch.

1. Enter **fwconfig**.

   The following prompt displays:

   ```
   Modify existing configuration? (y or n) (n) :
   ```

   Enter **y** to change the configuration.

2. The following prompt displays:

   ```
   Change authentication state to Disable? (y or n) (n) :
   ```

   Enter **y** to disable the software.

3. The following message displays:

   ```
   Firewall configuration change successful.
   Firewall is now disabled.
   ```

   The system prompt reappears.

4. If you decide to re-enable the software without rebooting first, you will see this message:

   ```
   Firewall started once before, switch must be rebooted to start again.
   ```

   You will be allowed to re-enable the software only *after* the switch reboots. The reason for this restriction is that the software in the switch cannot establish a reliable connection to the AMC after it has been disabled. The rebooting of the switch allows the software to reinitialize its connection to the AMC properly.

Moving an Authenticated Client Back to the Default Group

You can remove any user from an authenticated group by moving the user's MAC address back into the default group. Use the **avlDrop** command as described in Chapter 2, "RADIUS Authentication.

Troubleshooting Instructions

Below are some instructions intended to help you troubleshoot problems with client authentication. Refer to the release notes for additional help.

♦ Important Note ♦

In any troubleshooting situation, always make sure group mobility is enabled globally on the switch (using the **gmcfg** command) and that the default group and all authenticated groups have group mobility enabled (using the **gmstat** command). These commands are described in the "Managing Groups and Ports" chapter of your switch manual.

Telnet client does not work or telnet authentication fails. Make sure you are telnetting to the correct address and port using the **avlports** and **avlsports** commands as described in *Configuring Authenticated Ports* on page 1-18. The Telnet authentication address should be set up as described in *Setting Up Telnet Clients* on page 1-27. For example, if your authenticated network is group 2 (10.0.0.0), configured with an IP router port of 10.0.0.100, the default Telnet authentication address should be 10.0.0.253. The default Telnet port is always 259.

AMC Authentication fails. There may be a problem with Skey password sychronization because of the way the password was set up. On the AMC configure a new password by entering the new password for each of the remote modules corresponding to each of the switches. Verify that each of the switch names used in the configuration of each remote module and for each switch network object is the same as the name that is found in the Hosts file on the AMC. Restart the AMC. On the switch use the **fwconfig** command to configure the new Skey password.

Client authenticates but is not moved into the correct authenticated group. For AMC Authentication, make sure that you are using the correct Check Point license. If you use a Firewall-1 license rather than an Authentication license, the AMC may appear to work but the authentication client cannot access the correct group(s).

Authentication client does not remain in authenticated group. Make sure the MAC timeout is not expiring on the switch (using the **stc** or **syscfg** commands). Use the **macinfo** command to verify that the MAC address of the client belongs to the correct group.