Installation and Getting Started Guide

HP ProCurve Secure Access 700wl Series

www.hp.com/go/hpprocurve

HP PROCURVE
SECURE ACCESS 700WL SERIES

INSTALLATION AND GETTING STARTED GUIDE

Publication Number

5990-8806
March, 2004
Edition 1

Applicable Products

HP ProCurve Access Controller 720wl	(J8153A)
HP ProCurve Access Control Server 740wl	(J8154A)
HP ProCurve Integrated Access Manager 760wl	(J8155A)
HP ProCurve 700wl 10/100 Module	(J8156A)
HP ProCurve 700wl Gigabit-SX Module	(J8157A)
HP ProCurve 700wl Gigabit-LX Module	(J8158A)
HP ProCurve 700wl 10/100/1000Base-T	(J8159A)
HP ProCurve 700wl Acceleration Module	(J8160A)

Trademark Credits

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

CONTENTS

PREFACE

This preface describes the objective, audience, use, and organization of the *Installation and Getting Started Guide.* It also outlines the document conventions, related documentation, and support information.

Audience

The audience for this document is the network administrator who wants to enable network users to communicate using the 700wl Series system. This document is intended for authorized personnel who have previous experience working with network telecommunications systems or similar equipment. It is assumed that the personnel using this document have the appropriate background and knowledge to complete the procedures described in this document.

Document Objectives

This document contains procedural information describing the installation and configuration of the HP ProCurve Integrated Access Manager 760wl, Access Control Server 740wl, or Access Controller 720wl. Each procedure is written in a task-oriented format consisting of numbered step-by-step instructions. In most cases, several procedures are required to complete one overall task. All procedures should be performed in the order they appear in this document, unless otherwise instructed.

This document also provides instructions for the creation of a basic configuration of the HP ProCurve Secure Access 700wl Series that allows a user to:

- Connect to the 700wl Series system (optionally using a secure protocol (PPTP))
- Log in and be authenticated through the HP ProCurve 700wl Series built-in database
- Pass IP traffic and have access to network resources.

A system running with this configuration is suitable for basic evaluation or demonstration purposes.

Organization

This document is organized as follows:

Chapter 1— Introduction

This chapter gives an overview of the 700wl Series system installation procedure.

Chapter 2— Hardware Installation

This chapter describes the installation of the HP ProCurve Access Control Server 740wl, and Access Controller 720wl.

Chapter 3— Network Setup

This chapter describes the network configuration of the Access Control Server after it has been physically installed.

Chapter 4—Basic Configuration

This chapter leads you through the configuration of a basic system setup that provides user accounts and user authentication, as well as a PPTP gateway, and supports an external authentication service such as LDAP.

Appendix A—Troubleshooting

This chapter presents troubleshooting procedures for the 700wl Series system.

Appendix C—LCD Display Description

This appendix describes the LCD display on the Access Controller 720wl, Access Control Server 740wl, and Integrated Access Manager 760wl. The display can be used to view the system's network parameters, and to power down the system.

Appendix D—Technical Specifications, Safety and Compliance

This appendix describes the technical specifications of the system, and provides safety and compliance information.

Appendix E—Cable and Connector Specifications

This appendix describes the Serial Connector and the Standard Ethernet cables for use with the 700wl Series system.

Related Publications

The following lists related publications:

- HP ProCurve Secure Access 700wl Series Management and Configuration Guide, Software Release 4.0
- HP ProCurve 700wl Series Release Notes
- HP ProCurve 700wl Series Quick Start Guides

Document Conventions

The following text conventions are used in this document:

Convention	Definition
Boldface Arial	Screen menus that you click to select, field names, and commands that you select are in boldface Arial.
Italic Palatino	New terms that are defined in the text, and emphasized terms are in italic Palatino.
`Courier`	Filenames and commands or text that you type are in `Courier`.

The following icons are used to alert you to important information:

Icon	Notice Type	Alerts you to...
None	Note	Helpful suggestions or information that is of special importance in certain situations.
None	Caution	Risk of personal injury, loss of system functionality, or loss of data.
	Warning	Risk of severe personal injury, system damage, or irrecoverable loss of data.

Support Information

See the HP ProCurve Networking web site at `www.hp.com/go/hpprocurve`. Click on **technical support** and select **support services** for a list of available support resources and options for contacting HP.

1 INTRODUCTION TO THE HP PROCURVE 700WL SERIES

This chapter gives a brief description of the installation procedures for HP ProCurve 700wl Series products. It consists of the following sections

Overview

There are five products that make up the HP ProCurve 700wl Series:

- HP ProCurve Access Control Server 740wl
- HP ProCurve Access Controller 720wl
- HP ProCurve Integrated Access Manager 760wl

The physical installation of the hardware for any of these products is essentially the same, and is described fully in Chapter 2, “Hardware Installation”. The hardware installation is always performed first, before the network installation.

Centralized Administration of the 700wl Series system

Wireless network clients physically connect through Access Controllers, but authentication and rights administration for these clients is handled centrally from the Access Control Server. In addition, all configuration of the Access Controllers connected to the system is handled by the Administrative Console located in the Access Control Server. Once you have installed an Access Controller onto your network, you should not need to perform any administration functions directly on the Access Controller.

From the centralized Administrative Console on your Access Control Server you can perform the following configuration functions:

- Configure the 700wl Series system setup, including bridging, DHCP Network for NAT Clients, Forwarding of IP Address broadcasts, setting up HTTP proxies, configuring SNMP settings, and setting the system date & time
- Update the 700wl Series system software or return to a previous version
- Set up Wireless Data Privacy policy for clients using VPN protocols
- Set up authentication policies for how users authenticate themselves to the system
- Set up access policies to control what users can do over the network

- Set up Identity Profiles to put users in groups that share the same access policies
- Set up Connection Profiles that allow you to specify different Access Policies for users based on location, time of day, VLAN tags, and Authentication Policies
- Set up redundant Access Control Servers to provide failover

Additionally, the Administrative Console provides functions for monitoring the status of the system components, as well as monitoring clients logged onto the system and their sessions.

Order of Network Installation

The order of installation depends on the complement of equipment you wish to install. There are three basic configurations, and for each, there is an order of network installation as follows:

- Access Control Server 740wl with at least one Access Controller 720wl
- Integrated Access Manager 760wl only, with no Access Controller 720wls
- Integrated Access Manager 760wl with one or more additional Access Controller 720wls
- Two redundant Access Control Server 740wls with at least one Access Controller 720wl

Access Control Server With One or More Access Controllers

If you are installing an Access Control Server 740wl and one or more Access Controller 720wls, perform installation in the following order:

Step 1. Install the Access Control Server, following the steps in the *HP ProCurve 700wl Series Quick Start Guide* included in the Documentation Kit that came with the unit, or in Chapter 2, "Hardware Installation" in this manual.

Step 2. Perform the network setup for the Access Control Server, following the steps in "Access Control Server or Integrated Access Manager Setup" on page 3-2.

Step 3. Install the Access Controllers following the steps in the *HP ProCurve 700wl Series Quick Start Guide* or in Chapter 2, "Hardware Installation" in this manual.

Step 4. Once the Access Controller is recognized by the Access Control Server and appears in the Access Control Server Administrative Console, perform any additional setup required, following the steps in"Access Controller Setup" on page 3-14.

Integrated Access Manager Only

If you are installing an Integrated Access Manager 760wl only, perform installation in the following order:

Step 1. Install the Integrated Access Manager, following the steps in the *HP ProCurve 700wl Series Quick Start Guide* included in the Documentation Kit that came with the unit, or in Chapter 2, "Hardware Installation" in this manual.

Step 2. Perform the network setup for the Integrated Access Manager and its internal Access Controller, following the steps in "Access Control Server or Integrated Access Manager Setup" on page 3-2.

Integrated Access Manager With Additional Access Controllers

If you are installing an Integrated Access Manager 760wl with one or more Access Controllers, perform installation in the following order:

Step 1. Install the Integrated Access Manager, following the steps in the *HP ProCurve 700wl Series Quick Start Guide* included in the Documentation Kit that came with the unit, or in Chapter 2, "Hardware Installation" in this manual.

Step 2. Perform the network setup for the Integrated Access Manager and its internal Access Controller, following the steps in "Access Control Server or Integrated Access Manager Setup" on page 3-2.

Step 3. Install the additional Access Controllers following the steps in the *HP ProCurve 700wl Series Quick Start Guide*, or in Chapter 2, "Hardware Installation" in this manual.

Step 4. Once each Access Controller is recognized by the Integrated Access Manager and appears in the Integrated Access Manager Administrative Console, perform any additional setup required, following the steps in *"Completing the Installation" on page 3-18.*

Redundant Access Control Servers with One or More Access Controllers

Step 1. Install each Access Control Server, following the steps in the *HP ProCurve 700wl Series Quick Start Guide* included in the Documentation Kit that came with the unit, or in Chapter 2, "Hardware Installation" in this manual.

Step 2. Perform the network setup for each Access Control Server, following the steps in"Access Control Server or Integrated Access Manager Setup" on page 3-2.

Note the IP address and shared secret of the Access Control Server that you plan to designate as the Primary Access Control Server. Do not configure the Access Control Servers (yet) as redundant peers.

Step 3. Install the Access Controllers following the steps in the *HP ProCurve 700wl Series Quick Start Guide*, or in Chapter 2, "Hardware Installation" in this manual.

Configure the Access Controllers with the IP address and shared secret of the Primary Access Control Server.

Step 4. Once the Access Controller is recognized by the Primary Access Control Server and appears in the Access Control Server Administrative Console, perform any additional setup required, following the steps in *"Completing the Installation" on page 3-18.*

Step 5. On the Access Control Server that is to be the redundant (non-Primary) Access Control Server, set the shared secret to be the same as the Primary Access Control Server.

Step 6. On the Primary Access Control Server, configure redundancy, following the steps in Chapter 6, "Configuring the Network" in the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for software Version 4.0.

Tools and Information Required

To perform network installation for an Access Control Server, Access Controller, or Integrated Access Manager, the information defined in Table 1-1 may be required:

Note: *The information you gather here is required during configuration and is presented here as a reminder to find it before beginning the network installation.*

Table 1-1. Installation Parameters

Parameter	Form
Hostname (Fully-Qualified)	Not required. Must be fully-qualified if provided. Example: am21b.corp.com **Note:** A hostname is required only for an Access Control Server or Integrated Access Manager that will have a real Secure Socket Layer (SSL) certificate installed. If you install a signed SSL certificate, the hostname must match that on the SSL certificate.
Domain name	Defines the system's domain if a hostname is not provided. Optional. Example: xyzcorp.com
IP address	Can be configured as a static IP address or can be obtained via DHCP.
Subnet Mask	Defines the system's subnet range. Can be obtained via DHCP. Example: 255.255.255.0.
Gateway (router) IP address	Defines the default router. Can be obtained via DHCP.
Primary and Secondary DNS server IP addresses	Defines the location of the primary and backup DNS servers. Can be obtained via DHCP.
Shared Secret	Secret key used to establish trust relationship between an Access Control Server or Integrated Access Manager and an Access Controller. Alphanumeric string. The same the shared secret must be configured on each system. Not required for an Integrated Access Manager if no additional Access Controllers are used.

Many of these parameters can be supplied by the DHCP server if the system is configured to obtain its IP address via DHCP. If the system is configured to use a static IP address, then all the parameters shown in the table must be provided when the system is configured for network installation.

The following tools and equipment are required to install a 700wl Series system in a rack:

- Tape measure and level
- Number 2 Phillips screwdriver

HARDWARE INSTALLATION 2

This chapter describes the hardware installation of the following HP ProCurve products: Access Control Server 740wl, Access Controller 720wl, and Integrated Access Manager 760wl. You must be sure that the site requirements are met and carefully follow the procedures described to physically install the equipment.

This chapter consists of the following sections:

Hardware Description

This section describes the hardware features of the Integrated Access Manager 760wl, Access Controller 720wl, and Access Control Server 740wl. These products are designed for high-performance, high-density wiring-closet applications.

An Integrated Access Manager 760wl or Access Controller 720wl with a single four-port 10/100 Ethernet card all look as shown in Figure 2-1. Figure 2-2 shows an Access Control Server 740wl, which looks similar to an Integrated Access Manager or Access Controller, but does not include any option cards.

Figure 2-1. Integrated Access Manager 760wl or Access Controller 720wl

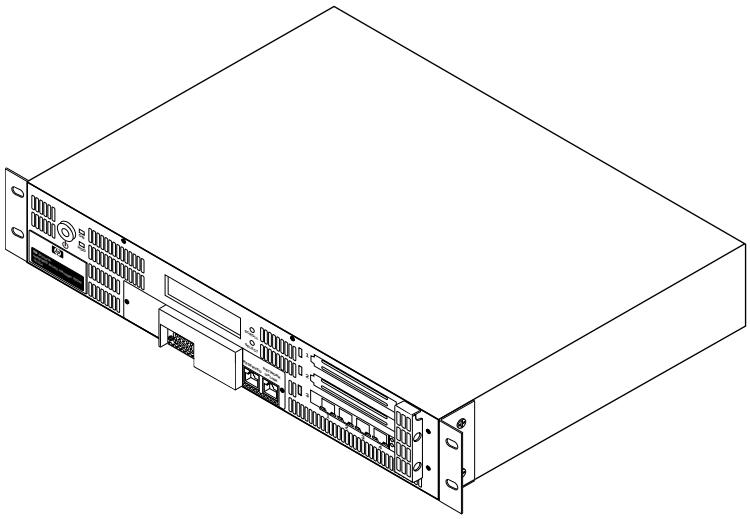
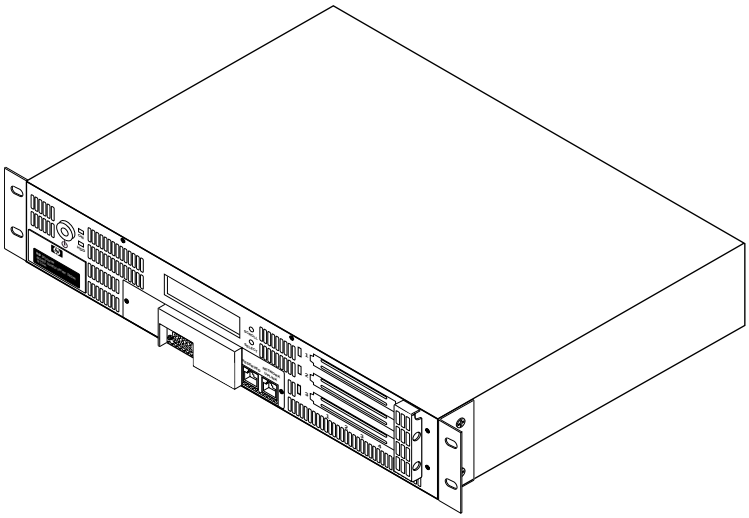


Figure 2-2. Access Control Server 740wl



The hardware for all three products is very similar, and consists of a chassis, power supply, fans, I/O ports, indicators, and switches. All systems have at least two RJ45 connectors—one for the network uplink, used to connect the system to the network, and one that is reserved for future use. Access Controllers and Integrated Access Managers may have up to twelve downlink access ports, used to connect wireless access points or other client-side devices to the system. Option cards with downlink ports can be pre-installed at the factory, or they can be ordered separately and added at a later time.

A front panel view of an Access Controller 720wl with a 4-port Ethernet card installed is shown in Figure 2-3. An Integrated Access Manager 760wl looks similar.

Figure 2-3. Front panel view—Integrated Access Manager 760wl or Access Controller 720wl

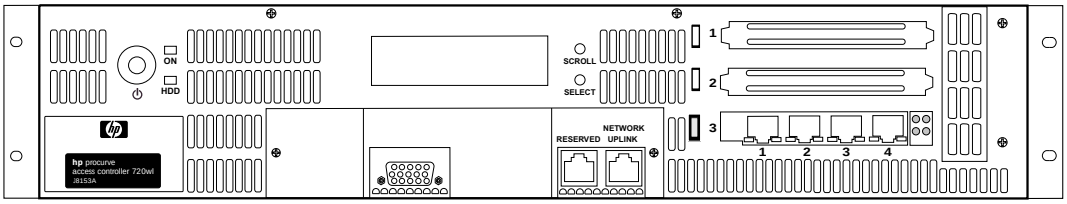
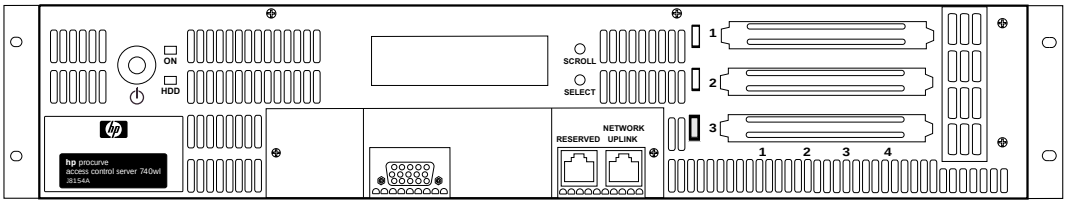


Figure 2-4 shows a front panel view of the Access Control Server 740wl.

Figure 2-4. Front panel view—Access Control Server 740wl



Note: *The system can optionally be configured to use an alternate port, such as a Fiber Gigabit Ethernet port on an option card, as the network uplink.*

System Memory/Storage

The Access Control Server 740wl and Integrated Access Manager 760wl are each equipped with a hard disk; the Access Controller 720wl is equipped with 256K of flash memory.

Figure 2-5 shows an Integrated Access Manager 760wl with the top cover removed. An Access Control Server 740wl looks similar, but without the riser board, into which option cards are inserted.

Figure 2-5. Integrated Access Manager 760wl with top cover removed

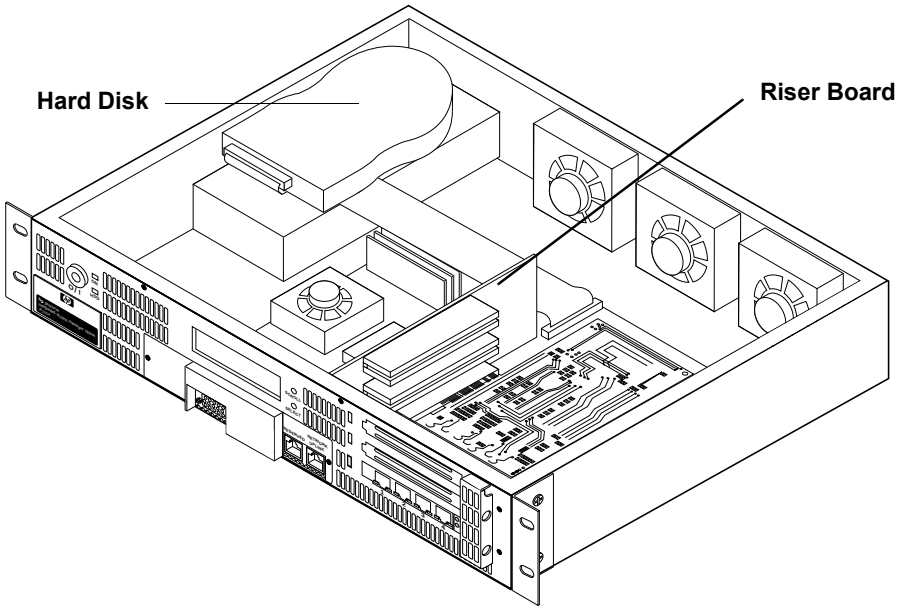
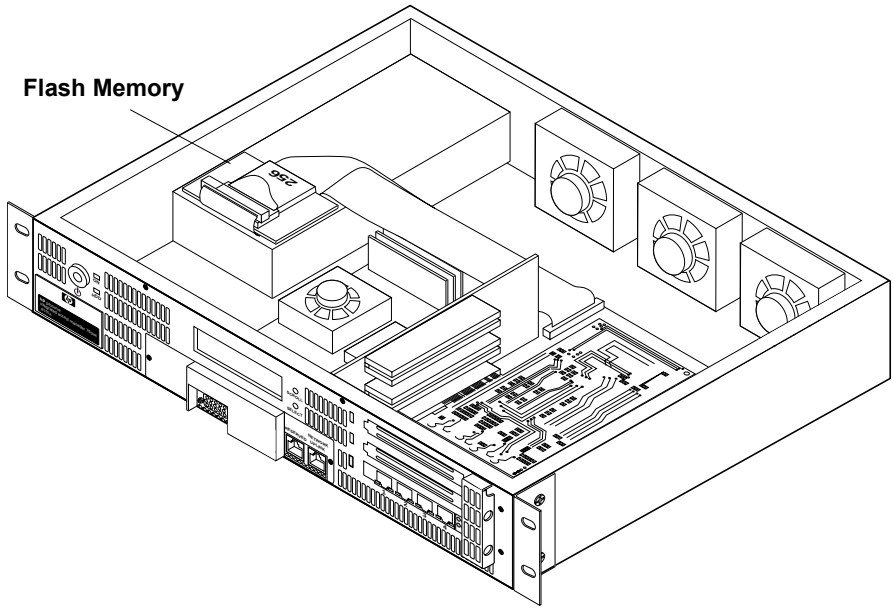


Figure 2-6 shows an Access Controller 720wl with the top cover removed.

Figure 2-6. Access Controller 720wl internal view



Chassis

The chassis is a 2 rack-unit (RU) enclosure, having dimensions 17.00″ (43.2 cm) wide, 15.00″ (38.1 cm) deep, and 3.5″ (8.9 cm) high. It weighs 14 lbs (6.4 kg). It can be mounted at the front with the brackets provided.

Power Supply

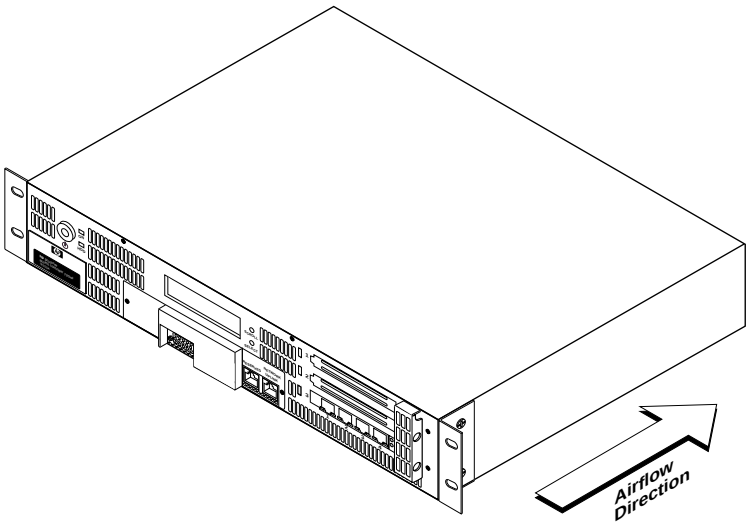
A single, non-redundant, auto voltage sensing power supply is provided. Input is 100-240 volts, 2.5A, 50/60 Hz, with a measured 87 watts output.

Fans

Note: *For environmental specifications, see "Site Power Requirements and Heat Dissipation".*

The system fan assemblies provide cooling air for the internal chassis components. The fans exhaust warm air from one end and draw in cool air at the other end. Figure 2-7 shows the direction of air flow through a 700wl Series unit.

Figure 2-7. Airflow direction



All 700wl Series systems monitor their internal fan speeds, internal chassis temperature, and power supply voltages. The status of these values are reported by system software.

I/O Ports

Table 2-1 summarizes the functional I/O ports on the Access Control Server 740wl, Integrated Access Manager 760wl and Access Controller 720wl.

Table 2-1. I/O Ports

Port Function	Description	Number of Ports		
		740wl	760wl	720wl
Network Uplink	RJ45, 10Base-T/ 100Base-TX/1000Base-T	1	1	1
Reserved port (for future use)	RJ45, 10Base-T/ 100Base-TX/1000Base-T	1	1	1
Serial Console	DB9, Serial Port	1	1	1
Access Controller Downlink Port	RJ45, 10Base-T/100Base-TX	0	up to 12	up to 12

Controls and Indicators

Controls

There is only one control on the front of the chassis, a power button, labeled I/0. The power button is a momentary switch and is used to turn on the system.

Note: *The front panel power button should not be used to power off the system. Turning off the system should be performed through software.*

There is also a power switch on the rear of the 700wl Series chassis, next to the power cord socket. This switch must be left in the On (I) position for the unit to be operational, and cannot be used to power on the system. When this switch is in the Off (0) position, the front panel power button will not function.

700wl Series units do not have a power switch on the back.

System Status Indicators

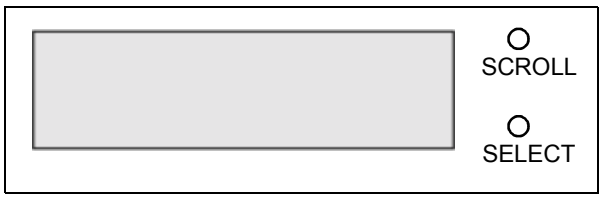
There are two system status LED indicators on the front of the chassis—Power (ON) and HDD.

- ON is lit when the power supply is plugged in to a live outlet, the rear panel On/Off switch is in the On position, and the power is turned on by the front panel On/Off button.
- HDD is lit when the internal hard disk drive is in use.

LCD Display

The display can be used to view the system's network parameters, and to power down the system. The LCD display is located in the middle of the front panel of 700wl Series products. It is a 16 character by two line display, with two buttons located to the right of the display (Figure 2-8).

Figure 2-8. LCD Display

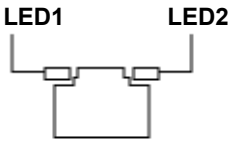


Appendix B, "LCD Display Description" describes the messages and operation of the LCD display panel.

Network Uplink Status Indicators

A detailed view of the network interface (uplink port) is shown in Figure 2-9.

Figure 2-9. Network Uplink port



The two LEDs, LED1 and LED2, provide information on the port speed and data connection state of the default network uplink port as shown in Table 2-2.

Table 2-2. Network uplink LED status

LED State	LED1 (Port Speed)	LED2 (Connection)
On	Orange: 100 Mbps Green: 1000 Mbps	Link established, Good connection
Off	10 Mbps	No link/no connection
Blinking	——	Transferring data

Access Controller and Integrated Access Manager Port Indicators

The access ports on an Access Controller or Integrated Access Manager are labeled 1 to 4, reading from left to right, as shown in Figure 2-10. Each Cluster LED corresponds to one port as shown.

Figure 2-10. Access port labeling on an Access Controller or Integrated Access Manager

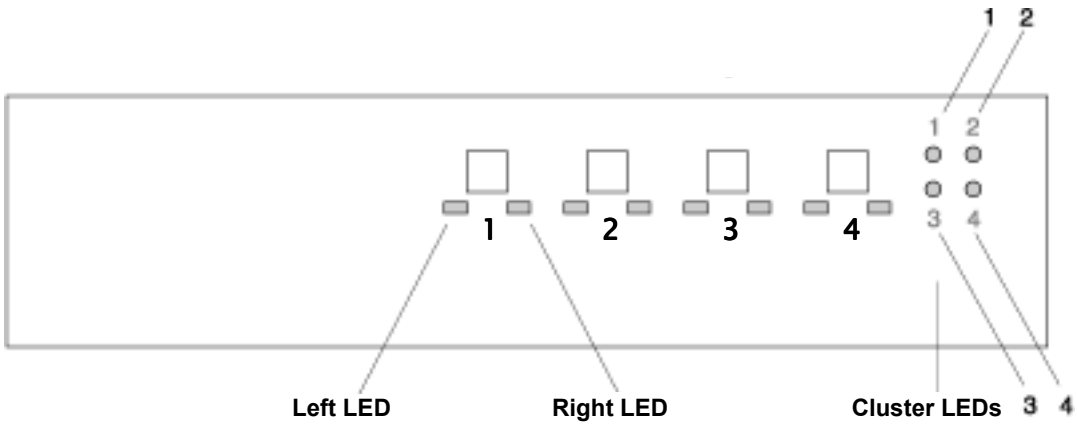


Table 2-3 shows the possible states for each LED and the meaning of each state.

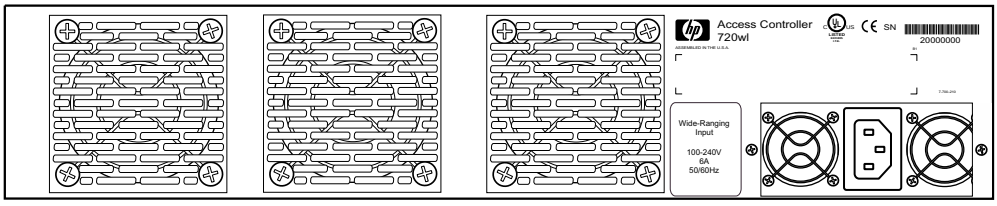
Table 2-3. Port LED Status Indicators

LED	State and Meaning
Left LED	**Off**: No activity **Blinking**: Data transfer
Right LED	**Off**: No link/no connection **On**: Link established, good connection
Cluster LEDs	Not used

Rear Chassis

Figure 2-11 shows the rear of the 700wl Series chassis. There are no controls on the rear of this chassis.

Figure 2-11. Rear chassis of a 700wl Series unit



Site Planning Checklist

Before installing an Integrated Access Manager 760wl, Access Control Server 740wl, or Access Controller 720wl, you should evaluate the items in the following site planning checklist:

Space Evaluation

- Space and layout
- Floor covering
- Impact and vibration
- Lighting
- Maintenance access

Environmental Evaluation

- Ambient temperature
- Humidity
- Altitude
- Atmospheric contamination
- Airflow

Power Evaluation

- Input power type
- Proximity of receptacle to equipment
- UPS for power failures

Grounding Evaluation

- Circuit breaker size

Cable and Interface Equipment Evaluation

- Cable type
- Connector type
- Cable distance limitations
- Interface equipment (transceivers)

EMI Evaluation

- Distance limitations for signaling
- Site wiring
- RFI levels

Site Power Requirements and Heat Dissipation

Table 2-4 shows the site power requirements and heat dissipation for the Integrated Access Manager 760wl, Access Control Server 740wl, and Access Controller 720wl.

Table 2-4. Site Power Requirements, Temperature and Heat Dissipation Parameters

Parameter	Value
Power Supply Output (Watts)	56
AC Input Power (Watts)	80
Heat Dissipation (BTU/Hr.)	170
AC Input Current at 120 VAC (Amps)	.88
AC Input Current at 240 VAC (Amps)	.44
Operating Temperature Range, °C	0 to 40
Storage Temperature Range, °C	-25 to +70
Humidity Range, non-condensing, percent	5 to 90

Installing a 700wl Series System

Note: *In this section, the hardware installation instructions for the Integrated Access Manager 760wl, Access Control Server 740wl and Access Controller 720wl are the same. Any of these is referred to as the "chassis."*

Unpacking

Unpack the contents carefully. Save the shipping containers and all packing materials. To save storage space, you may want to flatten the containers. Check that the following is included:

- Chassis
- Hardware and Accessories Kit
  - 12-24 x 5/8 inch Phillips pan-head bolts, zinc (quantity: 4)
  - 10-32 x 5/8 Phillips washer-head bolts, black (quantity: 4)
  - U.S. Power Cord
  - AT Null Modem (serial crossover) Cable (DB9 Female/DB9 Female)
- Documentation Kit
  - Documentation CD-ROM
  - Software License Agreement
  - Software Release Notes
  - HP ProCurve 700wl Series Quickstart Guide
  - HP ProCurve Secure Access 700wl Series Installation and Getting Started Guide (this document)

If any of the above is missing, contact HP immediately and do not attempt installation.

Rack Mounting the Chassis

Each 700wl Series chassis comes with attached L-brackets suitable for mounting the chassis in a standard 19-inch (48.3 cm) equipment rack with two unobstructed outer posts. This unit is not suitable for mounting in racks with obstructions (such as a power strip) that could impair access to the device. The air space in front and rear of system should be 6.00 in. minimum.

Caution: *Ground the chassis properly with the supplied power cord.*

Caution: *Be sure to position the power cord so that you can easily disconnect the chassis.*

Caution: *Do not install the chassis in an environment where the operating temperature might exceed 55˚C (123˚F).*

Caution: *Do not restrict air flow around the side and rear of the chassis. The air space in front and rear of system should be 6.00 in. minimum.*

Required Installation Tools

The following tools and equipment are required to install the chassis in a rack:

- Tape measure and level
- Number 2 Phillips screwdriver

Mounting Procedure

To install a chassis in a rack, follow these steps:

Step 1. Prepare for installation as follows:

a. Place the chassis on the floor or on a sturdy table, as close as possible to the rack. Leave enough clearance to allow yourself to move around the chassis.

b. Use the tape measure to measure the depth of the rack. Measure from the outside of the front mounting posts to the outside of the rear mounting strip. The depth must be at least 15.00 inches (38.1 cm).

c. Measure the space between the inner edges of the left front and right front mounting posts to ensure that it is 17.75 inches (45.09 cm) wide. The chassis is 17.00 inches (43.2 cm) wide and must fit between the mounting posts.

d. Open the accessories box and refer to the component checklist to verify that all parts are included, as described in "Unpacking".

Note: *Some equipment racks have a power strip along the length of one of the rear posts. If the rack has this feature, consider the position of the strip when planning fastener points.*

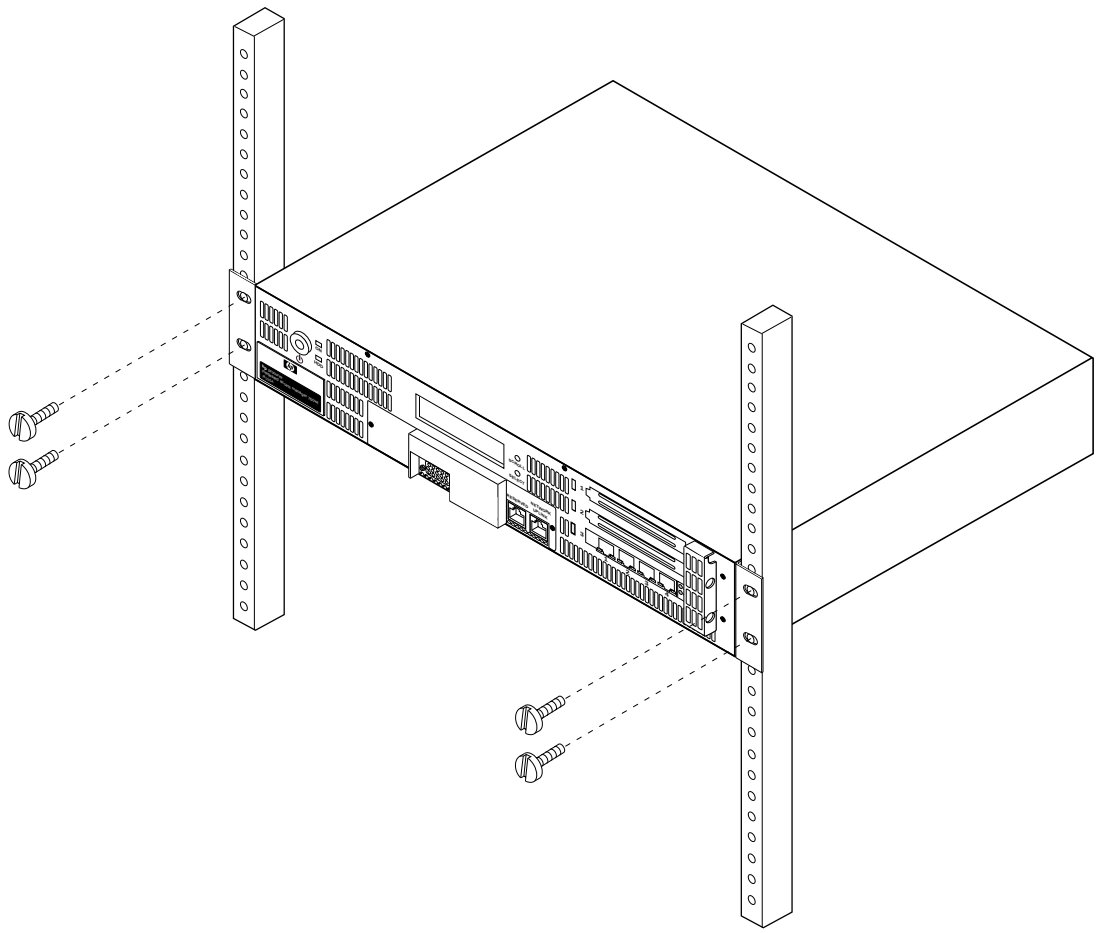
Step 2. Install the chassis in the rack as follows:

a. Align the mounting holes in the L-bracket with the mounting holes in the equipment rack.

b. Secure the chassis using either four 10-32 x 5/8 screws or four 12-24 x 5/8 screws (two per side) through the elongated holes in the L-bracket and into the threaded holes in the mounting post (Figure 2-12).

c. Use the tape measure and level to ensure that the chassis is installed straight and level.

Figure 2-12. Mounting the Integrated Access Manager 760wl in a rack or cabinet



Connecting Power to the Chassis

Follow these steps to connect power to the chassis:

Step 1. Before you connect the power supply to a power source, ensure that all site power and grounding requirements described above have been met.

Step 2. Plug the power cord into the rear of the chassis, as shown in Figure 2-11.

Step 3. Connect the other end of the power cord to an AC-power input source.

Adding an Option Card

Caution: *Be sure to wear a wrist grounding strap when installing an option card or otherwise working on the equipment with the cover removed. There is a danger of Electrostatic Discharge (ESD) damaging the equipment if this precaution is not taken.*

Warning: *Blank option card cover plates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, option card cover plates, front covers, and rear covers are in place.*

Warning: *High Voltages are present! Do not remove the cover until all power cables have been disconnected and the chassis is properly grounded. Failure to observe this may result in severe injury or death by electrocution.*

Removing the Top and Option Card Cover Plate

Step 1. Be sure that all cables have been removed, and attach a proper ESD wrist strap to your wrist.

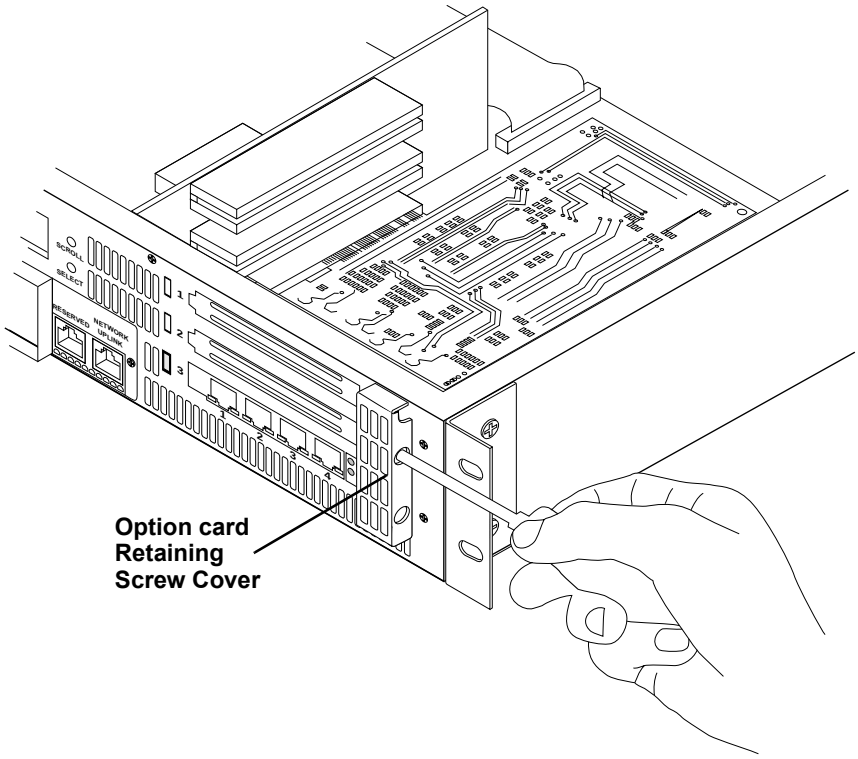
Step 2. Remove eight screws that secure the top cover to the chassis.

Step 3. Remove the cover.

Step 4. Using a #2 Phillips-head screwdriver inserted through the appropriate hole on the option card retaining screw cover, remove the screw holding the option card cover plate. Remove the option card cover plate from the front of the 700wl Series system (Figure 2-13).

Note: *A magnetic screwdriver may be useful, to help avoid screws falling into the unit, where they may be difficult to retrieve.*

Figure 2-13. Removing the option card cover plate

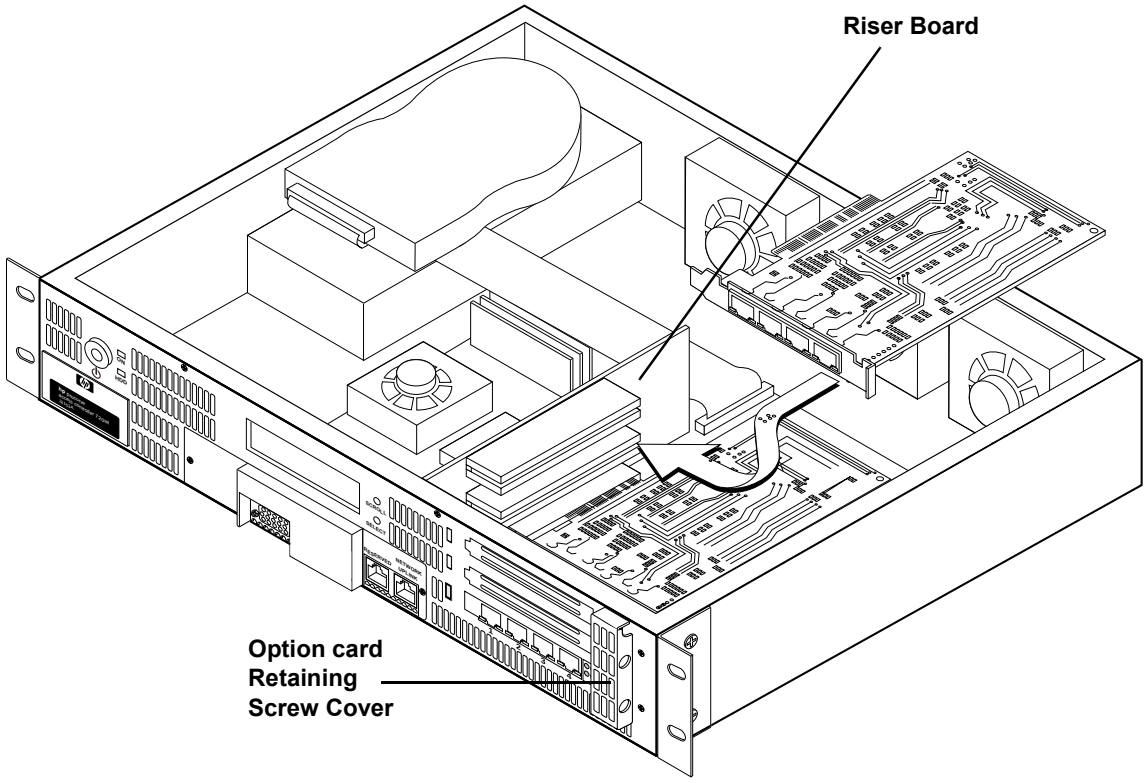


Inserting an Option Card into a 700wl Series Unit

Step 1. Remove the option card from its protective packaging, taking care not to damage it.

Step 2. Insert the card into the chassis as shown (Figure 2-14).

Figure 2-14. Inserting an option card into the 700wl Series chassis



Step 3. Be sure that the option card seats firmly.

Step 4. Using the screw removed with the option card cover plate, secure the option card to the chassis by inserting the screw and screwdriver through the option card retaining screw cover.

Step 5. Make sure the riser board is still perpendicular to the motherboard, and the option card is seated properly in and perpendicular to the riser board.

Step 6. Replace the cover, making sure the cover clips secure the riser board, and reinstall the eight screws holding the cover to the chassis.

Step 7. Reconnect the power cable.

Short Haul Fiber Gigabit Ethernet Option Card

To connect an SC cable to the Short Haul Fiber option card, use the LC-to-SC media converter shipped with the card. Make sure you remove the protective covers on the cable connectors before attempting to insert the connector into the card port, and before attempting to connect a cable to the female side of the media converter.

NETWORK SETUP 3

This chapter describes the network setup of your 700wl Series equipment on an existing network to allow interoperability and proper network security for all equipment.

It consists of the following sections:

Getting Started

The network configuration procedures in this chapter are performed after the hardware has been installed, as described in Chapter 2, "Hardware Installation". These network configuration procedures make a 700wl Series system (an Access Control Server or Integrated Access Manager and associated Access Controllers) usable on your network.

The Access Control Server or Integrated Access Manager must always be installed before any separate Access Controllers are installed. The network setup for an Integrated Access Manager is almost identical to the network setup for an Access Control Server. For simplicity many of the following steps reference only the Access Control Server, but apply to both an Access Control Server and an Integrated Access Manager.

700wl Series system components are configured and managed centrally from the Administrative Console that runs on the primary Access Control Server or the Integrated Access Manager. Therefore, the initial network configuration includes only the steps necessary to make the component accessible from the Access Control Server Administrative Console.

- For an Access Control Server or Integrated Access Manager, you may be able to access the Administrative Console immediately upon connecting the unit to your network, as the unit is configured by default to request an IP address using the Dynamic Host Configuration Protocol (DHCP). If a DHCP server is reachable, and an address is assigned to the HP ProCurve unit, you can point your browser to that IP address and access the Administrative Console. You can determine the IP address by looking at the LCD panel on the front of the unit.

  If you want to assign a static IP address to the unit, you can connect a serial console to the unit's serial console port, and assign an IP address prior to connecting the unit to the network. Once you have provided the necessary addressing information, you can connect via browser to the Administrative Console and complete the configuration.
- Management and configuration of an Access Controller is also performed from the centralized Administrative Console on the Access Control Server or Integrated Access Manager. However, in order for the Access Control Server and the Access Controller to communicate, the Access Controller must

first be configured with the IP address of the Access Control Server, and the shared secret used to validate the Access Controller to its Access Control Server. The Access Controller does not have a browser-based Administrative Console of its own, so this initial configuration must be done using the CLI via the serial console port.

Note: *If you plan to use an option card port (i.e a fiber gigabit port) as the network uplink port on an Integrated Access Manager or Access Controller, you must use the CLI to configure the uplink port, and you* ***must not connect the unit to your network*** *until after you have configured the uplink port. It is not possible to reconfigure the uplink using the browser-based Administrative Console.*

Access Control Server or Integrated Access Manager Setup

You can perform the initial network configuration of an Access Control Server in one of two ways:

- Connect a serial console to the Access Control Server's serial console port and use the Command Line Interface (CLI). See "Configuration Using the Command Line Interface" on page 3-3 for detailed instructions.
- Connect the Access Control Server to your network, allowing it to get an IP address using the Dynamic Host Configuration Protocol (DHCP). Then connect to its Administrative Console with a web browser. See "Configuration Using the Administrative Console" on page 3-7 for detailed instructions.

Configuration beyond basic network installation, i.e. the process of customizing the function of an HP ProCurve system to a particular end-user environment, is not described in this manual. Configuration performed after network installation is completed is described in the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide*.

Note: *The network setup for an Integrated Access Manager is identical to the network setup for an Access Control Server. For simplicity many of the following steps reference only the Access Control Server, but apply to both an Access Control Server and an Integrated Access Manager.*

IP Addressing Considerations

An Access Control Server or Integrated Access Manager requires a stable IP address so that the Access Controllers under its control can readily identify and communicate with the server. You can either arrange for DHCP to always assign the same IP address to the Access Control Server, or you can manually enter a static IP address. Most commonly, a static IP address is used.

A 700wl Series system ships configured by default to obtain its IP address and other information from a Dynamic Host Configuration Protocol (DHCP) server. This means the system will attempt to obtain an IP address as soon as it is connected to the network and is powered up.

Note: *If you do not want the Access Control Server to attempt to use DHCP, you must configure its IP address before you connect it to the network for the first time. You can configure the Access Control Server without connecting it to the network using a serial console connected to the serial port.*

If you do allow the Access Control Server to get its initial address using DHCP, this enables an administrator to connect to the Access Control Server's browser-based Administrative Console over the network to configure the system's other network parameters.

If you elect to obtain the Access Control Server IP address using DHCP, the Access Control Server can also obtain the hostname, domain name, subnet mask, default router address, and primary and secondary DNS server addresses from the DHCP server. Which information it receives depends on how you have configured your DHCP server.

If you configure your DHCP server to assign the same IP address to the Access Control Server every time, then even after a factory reset (which clears all configuration changes and returns the system to its default settings) the Access Control Server will obtain the correct IP address upon a reboot. If you elect to use a static IP address, you will need to reconfigure the address after a factory reset.

To install an Access Control Server or Integrated Access Manager onto a network, you need the information shown in Table 3-1:

Table 3-1. Installation parameters

Parameter	Description
Access Control Server hostname (optional)	Not required. Must be fully-qualified if provided. Example: am21b.corp.com
Domain name (optional)	Defines the Access Control Server's domain if a hostname is not provided. Optional. Example: corp.com
IP address	This can be assigned as a static IP address or can be obtained via DHCP (the default).
Subnet mask (Netmask)	Defines the Access Control Server's subnet range. Can be obtained via DHCP. Example: 255.255.255.0.
Gateway (default router) IP address	Defines the default router. Can be obtained via DHCP.
Primary and secondary DNS server IP addresses	Defines the location of the primary and backup DNS servers. Can be obtained via DHCP.
Integrated Access Manager only: Primary and secondary WINS server IP addresses	In a Windows environment where WINS servers are needed for client address resolution, defines the location of the primary and secondary WINS servers. Can be obtained via DHCP.
Access Control Server shared secret	Secret key used to establish trust relationship with an Access Controller. Alphanumeric string. The same shared secret must be configured on the Access Controller.

Configuration Using the Command Line Interface

Note: *If you want your system to receive its IP address via DHCP, and you do not plan to reconfigure the uplink port, you can simply connect the unit to your network. By default a new unit requests an address via DHCP. You can then follow the instructions in the section "Configuration Using the Administrative Console" on page 3-7. The remainder of this section assumes you plan to assign a static IP address to the unit.*

You can connect a serial console to the Access Control Server's serial console port, and then configure the Access Control Server's network settings using the CLI.

You can use the CLI to perform both basic and advanced network configuration on an Access Control Server or Integrated Access Manager. However, it is recommended that management and configuration

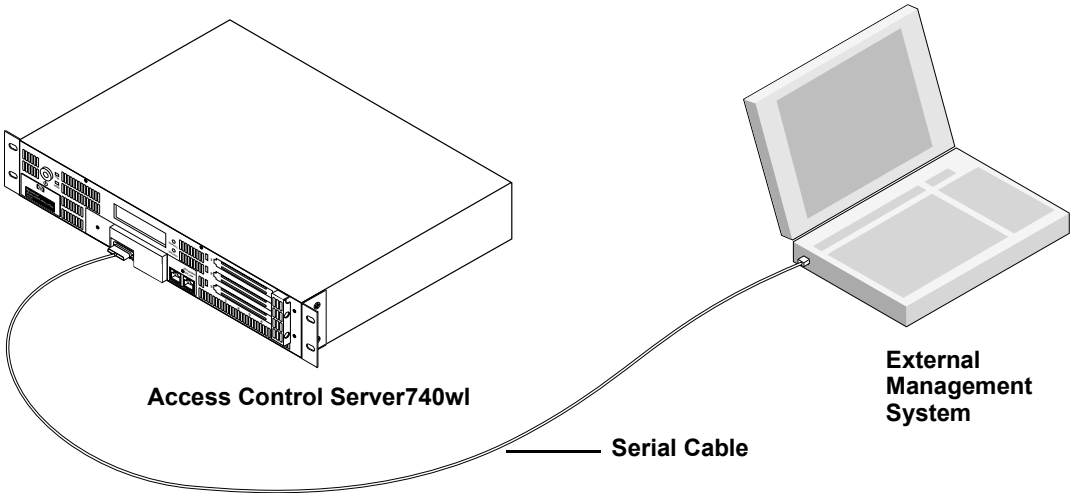
normally be done through the browser-based Administrative Console. Therefore, this section includes configuration of only those parameters necessary to allow the Access Control Server or Integrated Access Manager to be recognized and communicate on the network.

Note: *See Appendix A in the HP ProCurve Secure Access 700wl Series Management and Configuration Guide for full documentation of the commands available from the Command Line Interface (CLI).*

Connecting to a Serial Console

To use the CLI, you must first connect a cable from the serial port male DB9 connector on the Access Control Server to a serial console. (Figure 3-1).

Figure 3-1. Connecting an Access Control Server to a Serial Console



Typically, the serial console is a terminal emulator running on another management computer that is usually equipped with a male DB9 port. If your management computer is so equipped, you would use a female DB9 to female DB9 crossover serial cable (also known as a null modem cable) to connect the two devices. See Appendix D, "Cable and Connector Specifications" for the pinout specifications for this connector.

Configure the terminal session on your management computer as follows:

- Baud rate: 9600
- Data Bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

Caution: *If this is an Integrated Access Manager and you plan to reconfigure the network uplink to use a port on an option card,* ***DO NOT connect the unit to the network at this time****.*

Issuing Network Setup Commands from the Serial Console

After you have connected the serial console, follow these steps to configure the Access Control Server network parameters. These instructions assume you have not connected the unit to the network.

Step 1. Power up the Access Control Server. You will see a series of messages on the terminal emulator as the system boots and initializes itself.

At the end of the boot and initialization sequence you will see a prompt:

```
HP ProCurve Serial Console
Press return for console:
```

Step 2. Press **Return** and enter *admin* as the login id and *admin* as the initial password.

```
login:admin
Password: xxxxx
```

The system then displays the command prompt:

```
HP ProCurve Access Control Server #<MAC address>
HP 700wl Series@[0.0.0.0]:
```

Step 3. To configure the system with a static IP address, enter the following commands:

`set ip <ip address> <netmask>`

`<ip address>` is the IP address you want to assign to the Access Control Server. Make sure you assign an IP address that is valid for use as a device address. For example, IP addresses ending in .0 (xxx.xxx.xxx.0) are normally used as broadcast addresses and should not be used as a device address.

`<netmask>` is the subnet mask that defines the subnet address range for the Access Control Server. It must be entered in the format xxx.xxx.xxx.xxx — for example, 255.255.255.0.

`set hostname <fully qualified hostname>`

The hostname must be a valid, fully qualified name that correctly resolves to the IP address you assign to this Access Control Server. This parameter is optional.

`set gateway <ip address>`

`<ip address>` is the address of the default router.

`set dns <primary dns ip address> <secondary dns ip address>`

The two DNS IP addresses are the addresses of your primary and secondary DNS servers. The secondary IP address is optional.

Step 4. Change the administrator login and password by entering the following command:

`set admin <login-name> <password> <password>`

You must enter the password twice.

Step 5. Set the shared secret the Access Controllers will use to validate themselves to the Access Control Server as follows:

`set sharedsecret <secret> <secret>`

You must enter the shared secret twice.

Step 6. If you are configuring an Integrated Access Manager and you intend to use a port on an option card as the network uplink port, you must reconfigure the uplink port from the default on-board port (slot 0 port 2) to the port on the option card.

Caution: *Make sure the Integrated Access Manager is NOT connected to the network when you reconfigure the uplink port. Until you reconfigure the option card port as the uplink port, it functions as a downlink port; however, as soon as it is configured as the uplink port, the on-board (default) uplink port becomes a downlink port. If either of these ports is connected to the network while it is functioning as a downlink port, major network problems may occur.*

To reconfigure the uplink port, enter the following commands:

```
set uplink <slot>/<port>
```

`<slot>` is the slot in which the option card is installed, `<port>` is the port number. The port is always port 1 for a single-port card.

If the Access Control Server does not get its IP address through DHCP, set the IP address.

```
set ip <ip-address> [netmask]
reboot
```

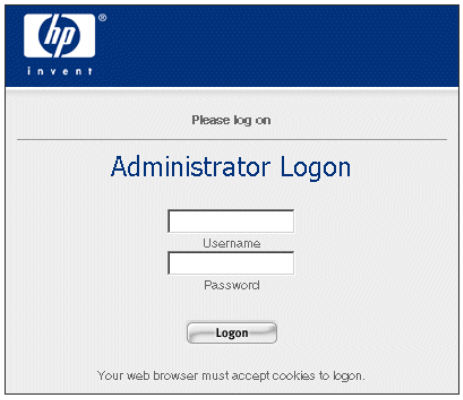
Step 7. Connect the Access Control Server Network Uplink port to your network. Figure 3-3 in the next section illustrates the connection of the default (on-board) Network Uplink port.

Step 8. Verify that you can access the Administrative Console from a browser running on a computer system connected to your network by entering the IP address of the unit:

```
http://<ip address>
```

The Administrator Logon page should appear (see Figure 3-2).

Figure 3-2. Administrator Logon



Step 9. Log on using the username and password you set in Step 4.

Step 10. You can now use the browser-based Administrative Console to complete the configuration of other settings such as advanced network features, session logging, SNMP management, the HTTP proxy feature, Wireless Data Privacy settings, and setting up authentication and access policies for client network access. For example, see Step 18 on page 3-13 in the section“Configuration Using the Administrative Console” for information on setting the system date, time and time zone.

See the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for detailed information on the features of the Administrative Console.

Configuration Using the Administrative Console

If you want to perform network installation of your Access Control Server using the browser-based Administrative Console, you must connect to the Access Control Server over the network. This requires that you know the IP address (or valid hostname) of your Access Control Server. Since the Access Control Server by default requests an IP address from a DHCP server, you can use the IP address assigned by the DHCP server to connect to the Administrative Console.

Before you connect your Access Control Server to the network, you can configure the DHCP server to provide a fixed IP address to the Access Control Server. If you do this, then the DHCP server can also provide the netmask, default gateway (router) IP address, and primary and secondary DNS IP addresses. You will only need to change the administrator user ID and password (strongly recommended) and configure the shared secret that enables Access Controllers to communicate with the Access Control Server.

If you cannot or do not wish to configure your DHCP server to provide a known address, then in order to connect to the Access Control Server you must determine the IP address supplied by DHCP. The easiest way to do this is by looking at the LCD display on the Access Control Server. The LCD alternates the display of the IP address with the display of the date/time and software version number.

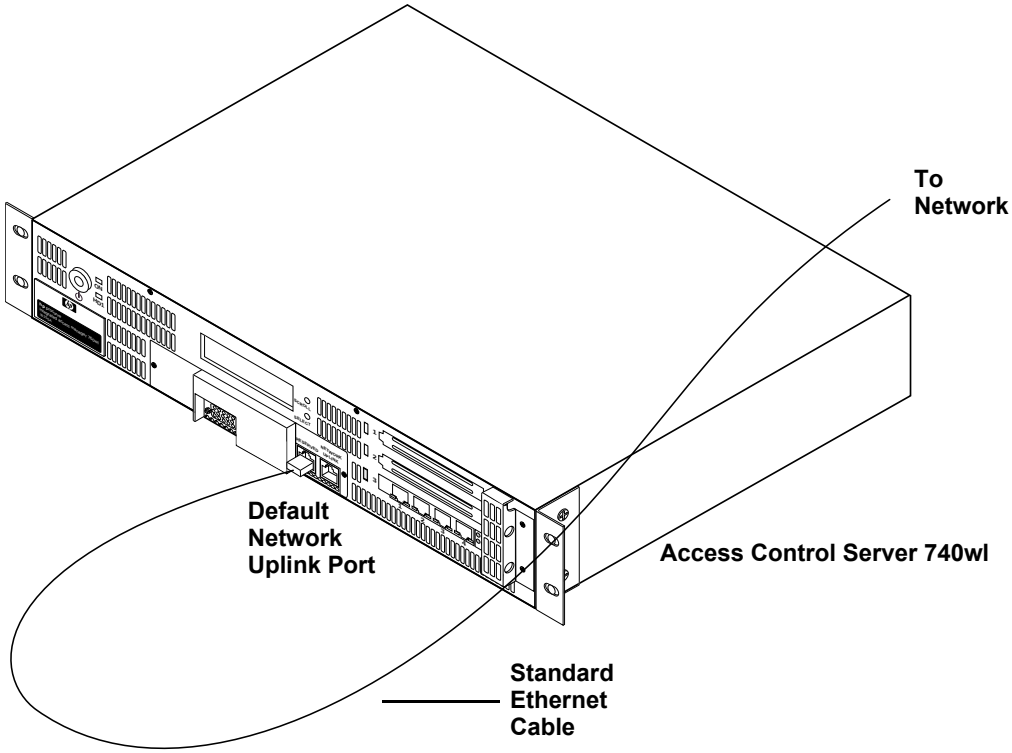
If you do not have access to the Access Control Server itself, you can find the IP address by examining the logs on your DHCP server to determine which address was given to the Access Control Server. An alternate method is to connect a serial console as described in "Configuration Using the Command Line Interface", and note the IP address that is contained as part of the CLI prompt.

Note: *If you plan to use a port on an option card as the network uplink port, you will need to use the serial console interface to change the network uplink port. The uplink port cannot be reconfigured through the browser-based Administrative Console. See "Configuration Using the Command Line Interface" and specifically Step 6 in the procedure, for instructions.*

Proceed as follows:

Step 1. Connect the Access Control Server Network Uplink port to your network, as shown (Figure 3-3).

Figure 3-3. Connecting the Access Control Server to the network through the default Network Uplink port



Step 2. Connect a web browser to the Access Control Server by entering a URL of the form:

`http://<ip address>`

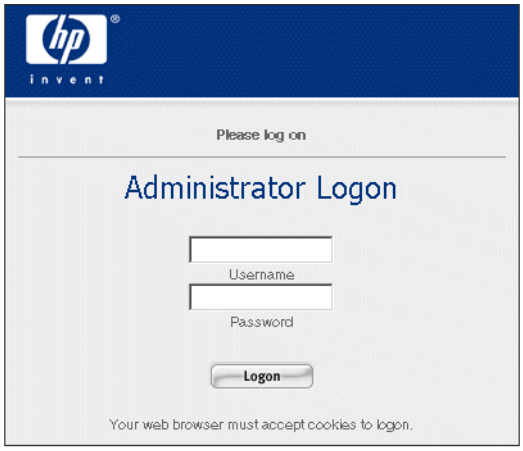
where `<ip address>` is the address assigned to the Access Control Server, or

`http://<fully-qualified hostname>`

if your DNS server is set to resolve the hostname to the IP address provided by your DHCP server.

The Administrator Logon page appears (Figure 3-4).

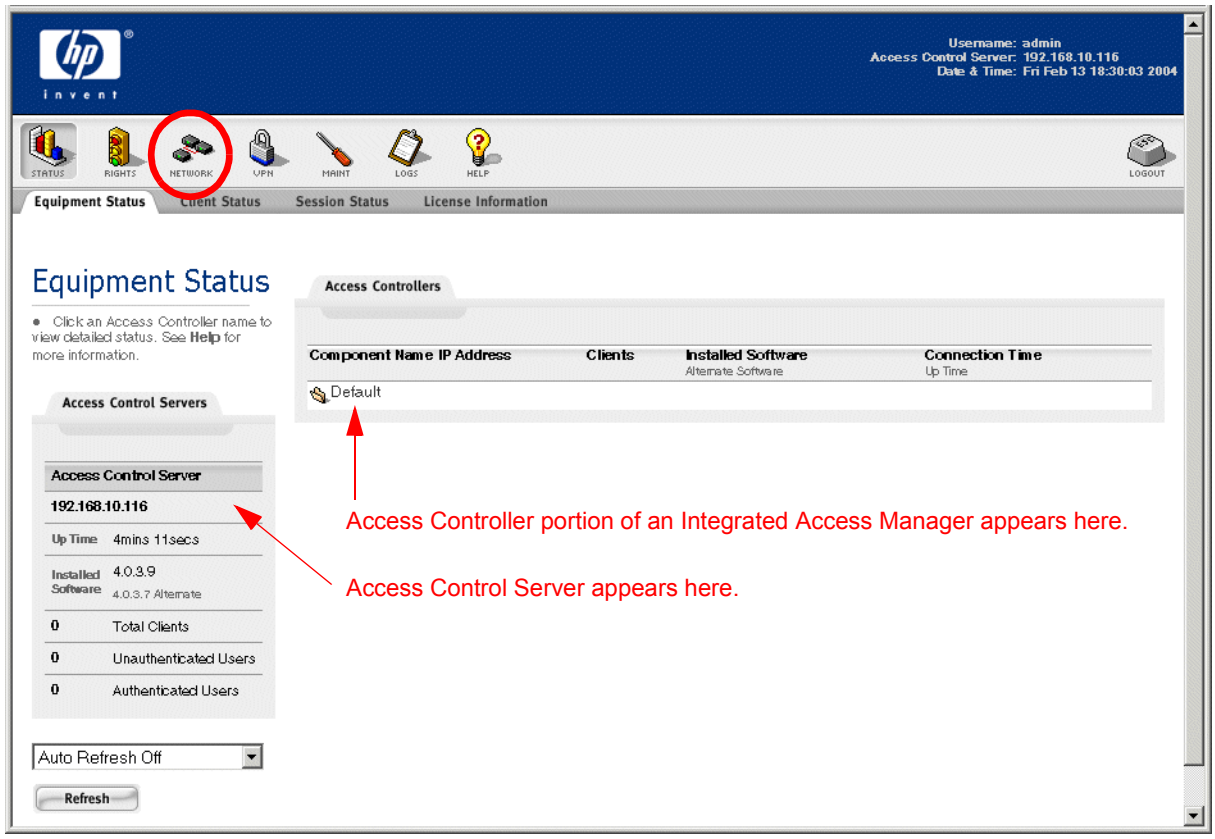
Figure 3-4. Administrator Logon



Step 3. For both the username and password, enter *admin*, and click **Logon**. The initial Administrative Console page appears, as shown in Figure 3-5.

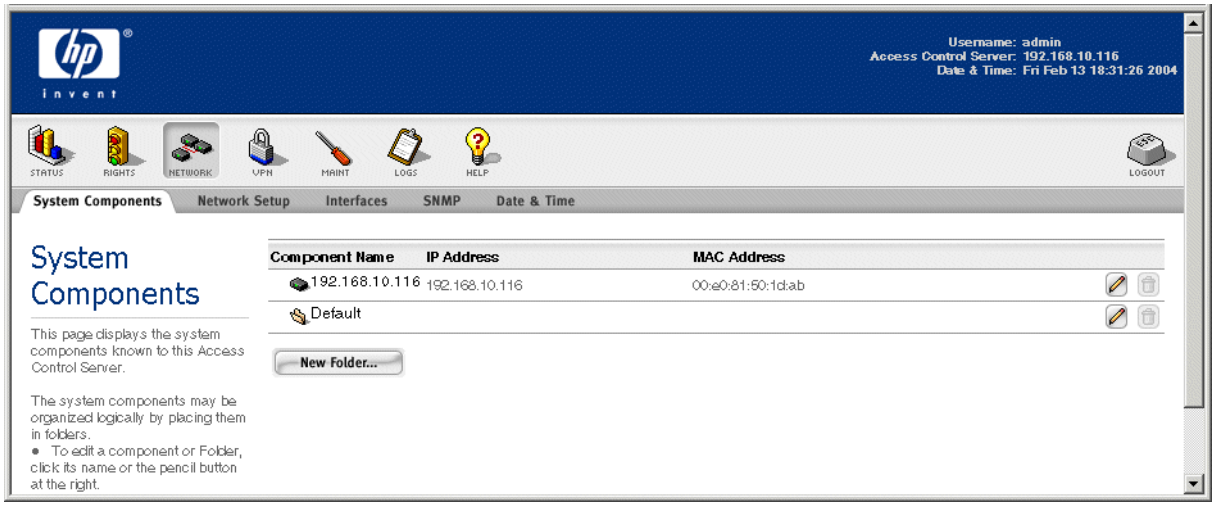
The Access Control Server will appear in the left hand column. If you are installing an Integrated Access Manager, the Access Controller portion of the Integrated Access Manager should appear in the Access Controllers list.

Figure 3-5. Initial Administrative Console page (Equipment Status)



Step 4. Click the **NETWORK** button (shown circled above). The System Components page appears, as shown in Figure 3-6.

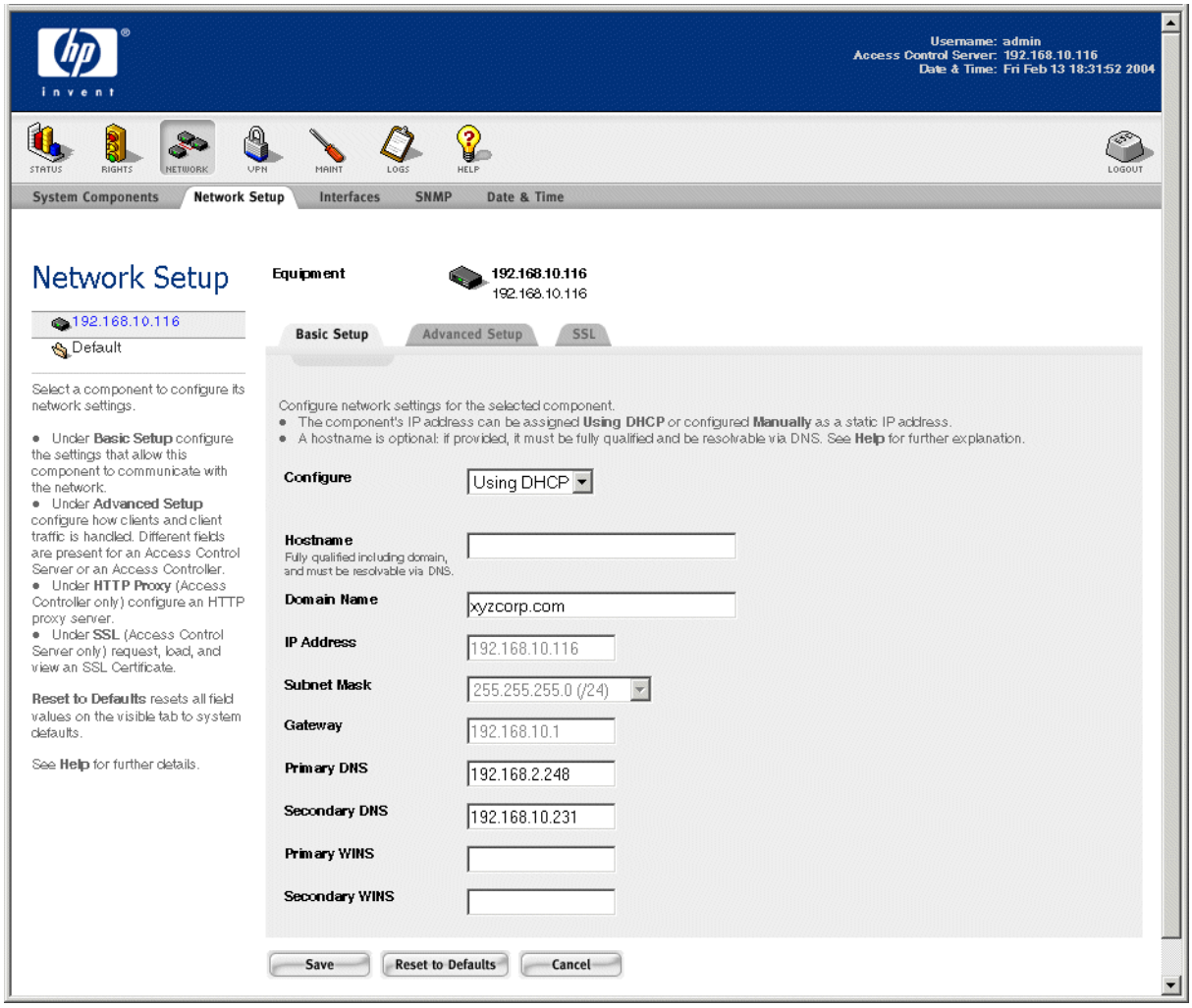
Figure 3-6. System Components page showing a newly-installed Access Control Server



If you are installing an Integrated Access Manager, the Access Controller portion will also appear in this display.

Step 5. Click the **Network Setup** tab just below the row of function buttons. This brings up the Network Setup page (see Figure 3-7).

Figure 3-7. Network Setup page for an Access Control Server



Step 6. If appropriate, enter a fully-qualified hostname for this Access Control Server.

Step 7. Enter the name of the domain in which this Access Control Server resides.

Step 8. If you choose to use DHCP to obtain an IP address for this unit, leave the **Configure** field set to **Using DHCP**, then enter any necessary values not supplied by the DHCP server in the appropriate fields on this page. If your DHCP server is configured appropriately, the IP address, subnet mask (netmask), gateway, and primary and secondary DNS addresses will already be filled in.

When using DHCP, you cannot change the IP address, subnet mask, or Gateway (default router) setting. You can change the DNS and WINS server IP addresses, if necessary.

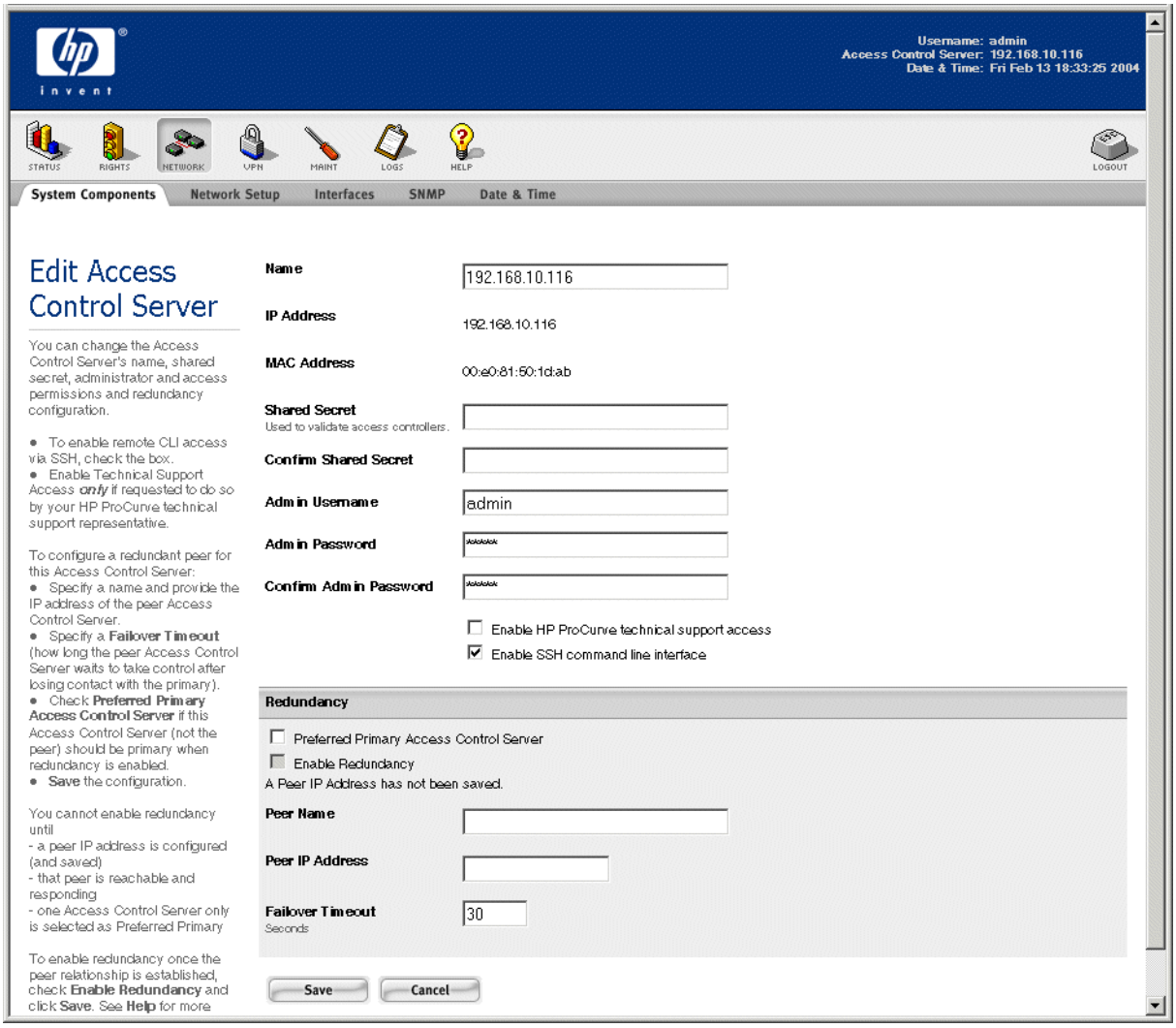
Step 9. If you want to set a static IP address, select **Manually** from the drop-down list of options for the **Configure** field, then enter the IP address, subnet mask, default router address, primary and secondary DNS server and primary and secondary WINS server IP addresses, as appropriate, in the fields on this page.

Step 10. Click **Save**.

Step 11. Return to the System Component page (Figure 3-6), and click the IP address link for the Access Control Server in the top row under System Components column. (If you are configuring an Integrated Access Manager, the Access Controller portion will be listed below the Access Control Server).

The Edit Access Control Server page appears (Figure 3-8). The Edit Integrated Access Manager page looks similar, but does not include the Redundancy area, as an Integrated Access Manager cannot function as a redundant peer.

Figure 3-8. Edit Access Control Server page



Step 12. To give the Access Control Server a descriptive name, replace the IP address in the **Name** field with the name you want to use.

Step 13. In the **Shared Secret** field, type the shared secret that Access Controllers will use to validate themselves to this Access Control Server.

Step 14. Retype the shared secret in the **Confirm Shared Secret** field.

Step 15. Change the administrator username and password by typing a new username and password, and confirming the new password in the appropriate fields.

Step 16. If you want to allow remote access to the CLI on this unit via a remote SSH client, leave the check in the **Enable SSH command line interface** box (this is the default). To disable remote access, uncheck the box.

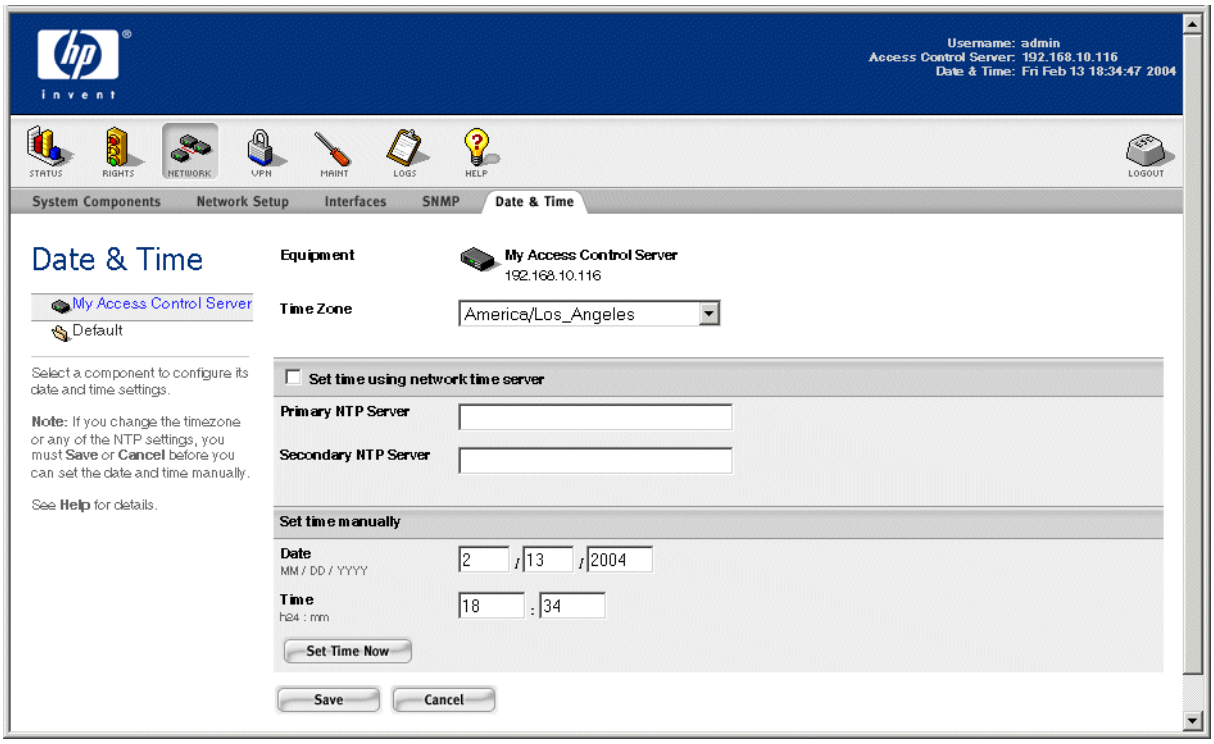
Enable technical support access only if requested to do so by an authorized HP ProCurve support engineer.

Step 17. Click **Save**.

Note: *You must enter and confirm a shared secret—the 700wl Series system does not let you save this configuration without one.*

Step 18. To set the system date and time, and time zone, if necessary, click the **Date & Time** tab. The Date & Time page appears (see Figure 3-9).

Figure 3-9. The Date & Time page



Step 19. To set the time zone, select the appropriate setting from the drop-down list.

Step 20. To configure an NTP server, click the **Set time using network time server** checkbox, and type the IP address of a primary and (optionally) a secondary NTP server.

Step 21. Click **Save**.

Step 22. To set the date and time immediately, select the appropriate values and click **Set Time Now**.

Note: *You cannot set the time zone or NTP server in the same operation occurrence as manually setting the time.*

This completes the basic configuration of an Access Control Server or Integrated Access Manager. You can now configure Access Controllers to communicate with this Access Control Server using the IP address and shared secret set in the previous steps.

To complete the configuration of the 700wl Series system, you will need to configure other settings such as advanced network features, session logging, SNMP management, the HTTP proxy feature, Wireless Data Privacy settings, and setting up authentication and access policies for client network access.

See the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for detailed information on the features of the Administrative Console.

Access Controller Setup

Configuration of an Access Controller is done primarily through the Administrative Console running on the Access Control Server to which the Access Controller is associated. However, in order for an Access Controller to be recognized by the Access Control Server, the Access Controller must be configured with the Access Control Server's IP address and shared secret. Until this is done, the Access Control Server and Access Controller will not be able to communicate. However, an Access Controller does not provide its own browser-based Administrative Console, as it is normally managed through the Access Control Server. Therefore, the initial configuration must be done through the CLI.

To do the initial configuration, you must connect a serial console to the Access Controller's serial console port, and configure the necessary settings using the CLI. The Access Controller does not need to be connected to the network. You cannot do the initial configuration of an Access Controller over the network.

IP Addressing Considerations

An Access Controller requires a stable IP address so that the Access Control Server can readily identify and communicate with it. You can either arrange for DHCP to always assign the same IP address to the Access Controller, or you can manually enter a static IP address. Most commonly, a static IP address is used.

A 700wl Series system ships configured by default to obtain its IP address and other information from a Dynamic Host Configuration Protocol (DHCP) server. This means the system will attempt to obtain an IP address as soon as it is connected to the network and is powered up. You can then reconfigure the system to use a static IP address, if desired.

Note: *If you do not want the Access Controller to attempt to use DHCP, you should configure its IP address before you connect it to the network for the first time.*

If you elect to obtain the Access Controller IP address using DHCP, the Access Controller can also obtain the hostname, domain name, subnet mask, default router address, primary and secondary DNS server, and (if needed) primary and secondary WINS server addresses from the DHCP server. The information it receives depends on how you have configured your DHCP server.

If you configure your DHCP server to assign the same IP address to the Access Controller every time, then even after a factory reset (which clears all configuration changes and returns the system to its default settings) the Access Controller will obtain the correct IP address upon a reboot. If you elect to use a static IP address, you will need to reconfigure the address after a factory reset.

To install an Access Controller onto a network, you need the information shown in Table 3-2.

Table 3-2. Installation parameters

Parameter	Description
Access Controller IP address	This can be assigned as a static IP address or can be obtained via DHCP.
Subnet mask (Netmask)	Defines the Access Control Server's subnet range. Can be obtained via DHCP. Example: 255.255.255.0.
Gateway (default router) IP address	Defines the default router. Can be obtained via DHCP.
Primary and secondary DNS server IP addresses	Defines the location of the primary and backup DNS servers. Can be obtained via DHCP.
Access Control Server IP Address	The IP address of the Access Control Server that will manage this Access Controller. In an environment with redundant Access Control Servers, this must be the IP address of the Primary Access Control Server.
Access Control Server shared secret	Secret key used to establish trust relationship between the Access Control Server and an Access Controller. Alphanumeric string. This must match exactly the shared secret configured on the Access Control Server.

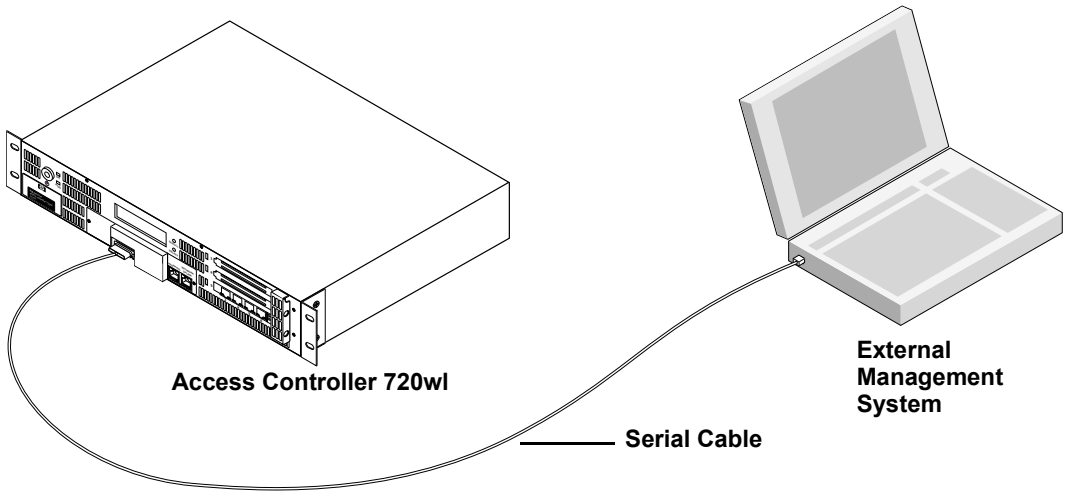
Configuration Using the Command Line Interface

Because an Access Controller does not provide its own browser-based Administrative Console, the initial system configuration must be done using the CLI via the serial console.

Connecting to a Serial Console

To use the CLI, you must first connect a cable from the serial port male DB9 connector on the Access Controller to a serial console. (Figure 3-1).

Figure 3-10. Connecting an Access Controller to a Serial Console



Typically, the serial console is a terminal emulator running on another management computer that is usually equipped with a male DB9 port. If your management computer is so equipped, you would use a female DB9 to female DB9 crossover serial cable (also known as a null modem cable) to connect the two devices. See Appendix D, "Cable and Connector Specifications" for the pinout specifications for this connector.

Configure the terminal session on your management computer as follows:

- Baud rate: 9600
- Data Bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

Note: *Do not connect the Access Controller to the network at this time.*

Issuing Network Setup Commands from the Serial Console

Note: *See Appendix A in the HP ProCurve Secure Access 700wl Series Management and Configuration Guide for a complete list of commands available for the Command Line Interface (CLI).*

After you have connected the serial console., follow these steps to configure the Access Controller network parameters:

Step 1. Power up the Access Controller. You will see a series of messages as the system boots and initializes itself.

At the end of the boot and initialization sequence you will see a prompt:

```
HP ProCurve Serial Console
Press return for console:
```

Step 2. Press **Return** and enter *admin* as the login id and *admin* as the initial password.

```
login:admin
Password: xxxxx
```

The system then displays the command prompt:

```
HP ProCurve Access Controller #<MAC address of Access Controller>
HP 700wl Series@[0.0.0.0]:
```

If you are using DHCP to supply the IP address, netmask, default router, DNS and WINS server IP addresses, go to Step 4. Otherwise, perform Step 3.

Step 3. Enter the following commands:

`set ip <ip address> <netmask>`

`<ip address>` is the IP address you want to assign to the Access Controller. `<netmask>` is the subnet mask that defines the subnet address range for the Access Controller. It must be entered in the format xxx.xxx.xxx.xxx — for example, 255.255.255.0.

`set hostname <fully qualified hostname>`

The hostname must be fully qualified, and it must resolve to the IP address you assign to this Access Controller. This parameter is optional.

`set domainname <domainname>`

`<domainname>` is the domain name for the Access Controller. This parameter is optional

`set gateway <ip address>`

`<ip address>` is the address of the default router.

`set dns <primary dns ip address> <secondary dns ip address>`

The two DNS IP addresses are the addresses of your primary and secondary DNS servers. The secondary IP address is optional.

Step 4. Set the IP address and shared secret of the Access Control Server as follows:

`set controlserver <ip address>`

`<ip address>` is the IP address of the Access Control Server that manages this Access Controller.

`set sharedsecret [<secret> <secret>]`

`<secret>` must match exactly the secret configured on the Access Control Server.

If you enter this command without its arguments, you are prompted for the shared secret and its confirmation.

Step 5. If you intend to use a port on an option card as the network uplink port, you must reconfigure the uplink port from the default on-board port (slot 0 port 2) to the port on the option card.

Caution: *Make sure the Access Controller is NOT connected to the network when you reconfigure the uplink port. Until you reconfigure the option card port as the uplink port, it functions as a downlink port; and as soon as it is configured as the uplink port, the on-board (default) uplink port becomes a downlink port. If either of these ports is connected to the network while it is functioning as a downlink port, serious problems can occur.*

To reconfigure the uplink port, enter the following commands:

`set uplink <slot>/<port>`

<slot> is the slot in which the option card is installed, <port> is the port number. The port is always port 1 for a single-port card.

If the Access Control Server does not get its IP address through DHCP, set the IP address.

```
set ip <ip-address> [netmask]
reboot
```

Step 6. With the serial console still connected, enter the command:

```
show ip
```

and verify that the information displayed is correct.

Step 7. You can now disconnect the serial console.

Step 8. Complete the installation as described in the next section, "Completing the Installation".

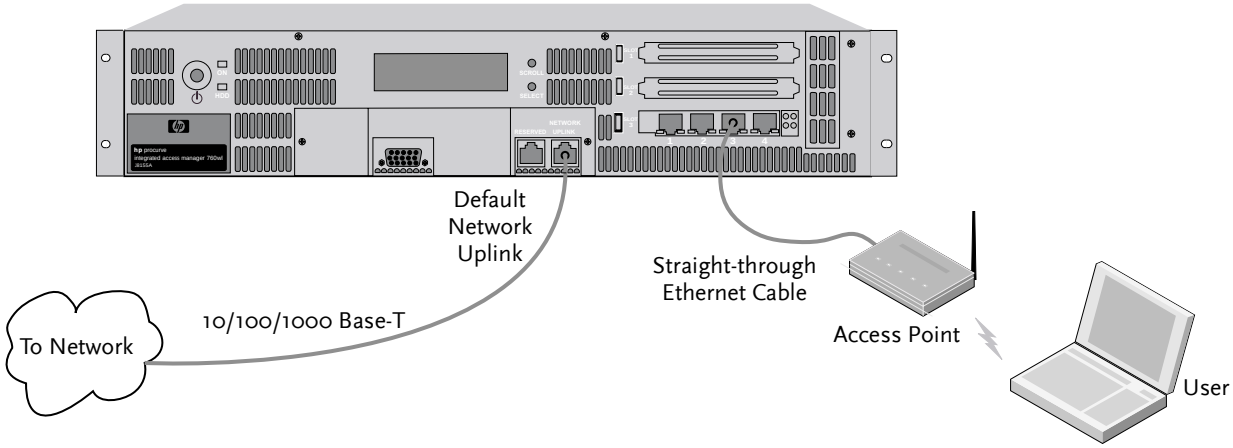
Completing the Installation

You can complete the configuration of your Access Controller through the Administrative Console running on the Access Control Server or Integrated Access Manager to which the Access Controller is associated.

Note: *Beyond the basic setup, all Access Controller configuration must be done through the Access Control Server Administrative Console. There is no browser-based Administrative Console provided on an Access Controller.*

If you have configured the Access Controller offline (while disconnected from the network) you must first connect the unit to your network using the Network Uplink port and a standard 10Base-T/100Base-TX/1000Base-T Ethernet cable. Figure 3-11 illustrates both the network uplink connection (via the default Network Uplink port) and the connection of a wireless Access Point to a downlink port.

Figure 3-11. Network uplink and wireless access point connections on an Access Controller.



If the system was configured to obtain an IP address from a DHCP server, then it should obtain one within 10-20 seconds after connecting to the IP network.

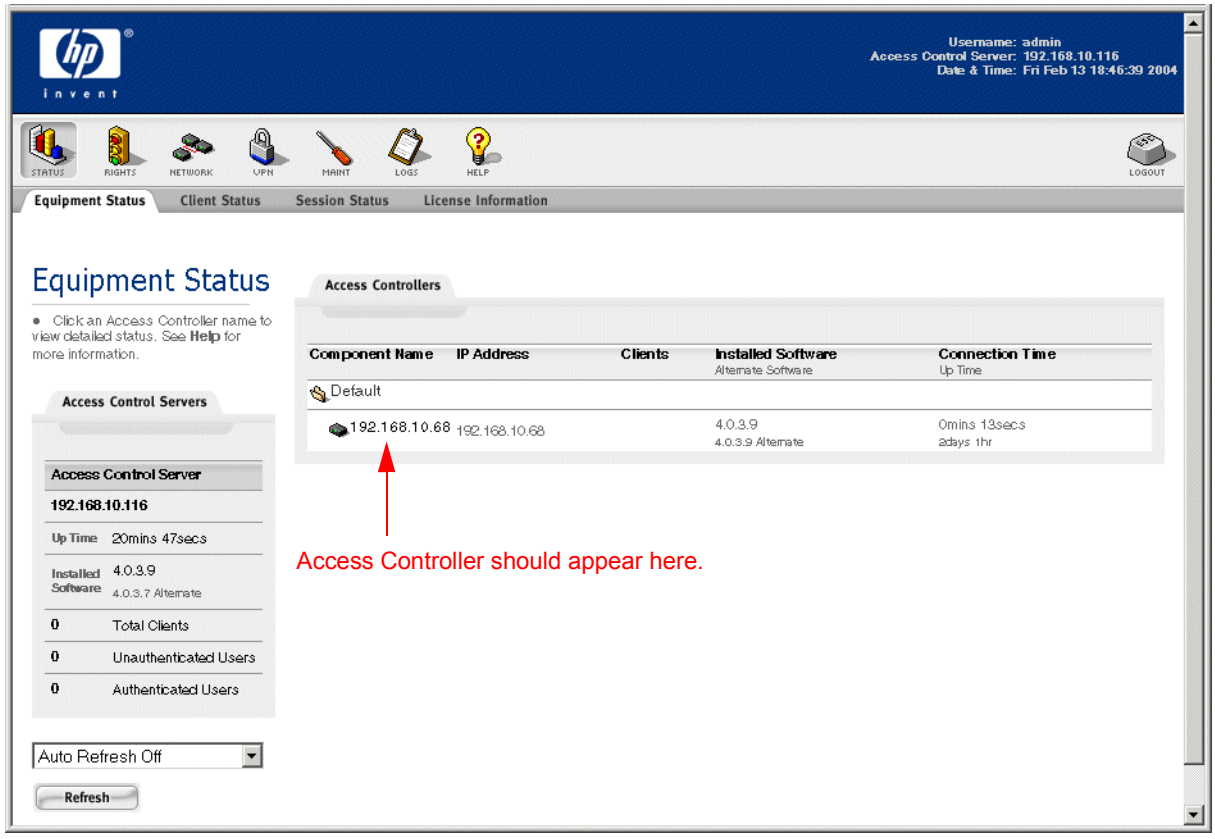
After a short period of time, the Access Controller should initiate communication with the Access Control Server. Once this has occurred, the Access Controller should appear as a system component in the Access Control Server's Administrative Console.

Note: *You can access online Help from within the Administrative Console at any time by clicking the* **HELP** *button. This displays a separate window containing Help about the page you are viewing.*

Step 1. Connect your browser to the Access Control Server or Integrated Access Manager whose address and shared secret you entered in Step 4 above, and log on to the Administrative Console.

Step 2. When the initial Administrative Console page appears, (the Equipment Status page, as shown in Figure 3-12) verify that this Access Controller appears under the list of Access Controllers.

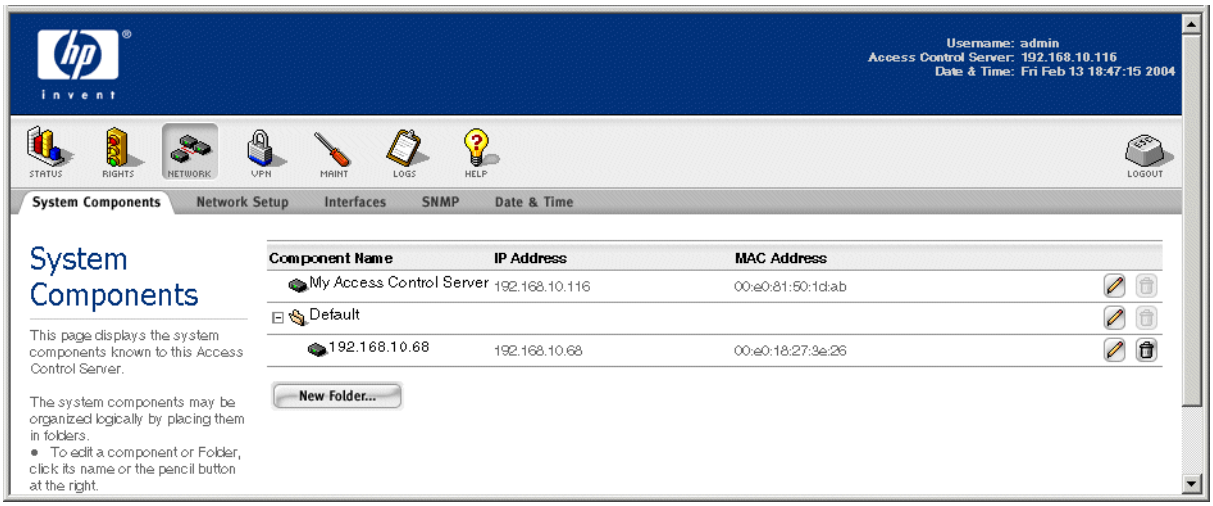
Figure 3-12. Initial Administrative Console page (Equipment Status)



Step 3. You can now use the Administrative Console to complete the configuration of other Access Controller settings such as setting the system time and date, and configuring other necessary settings:

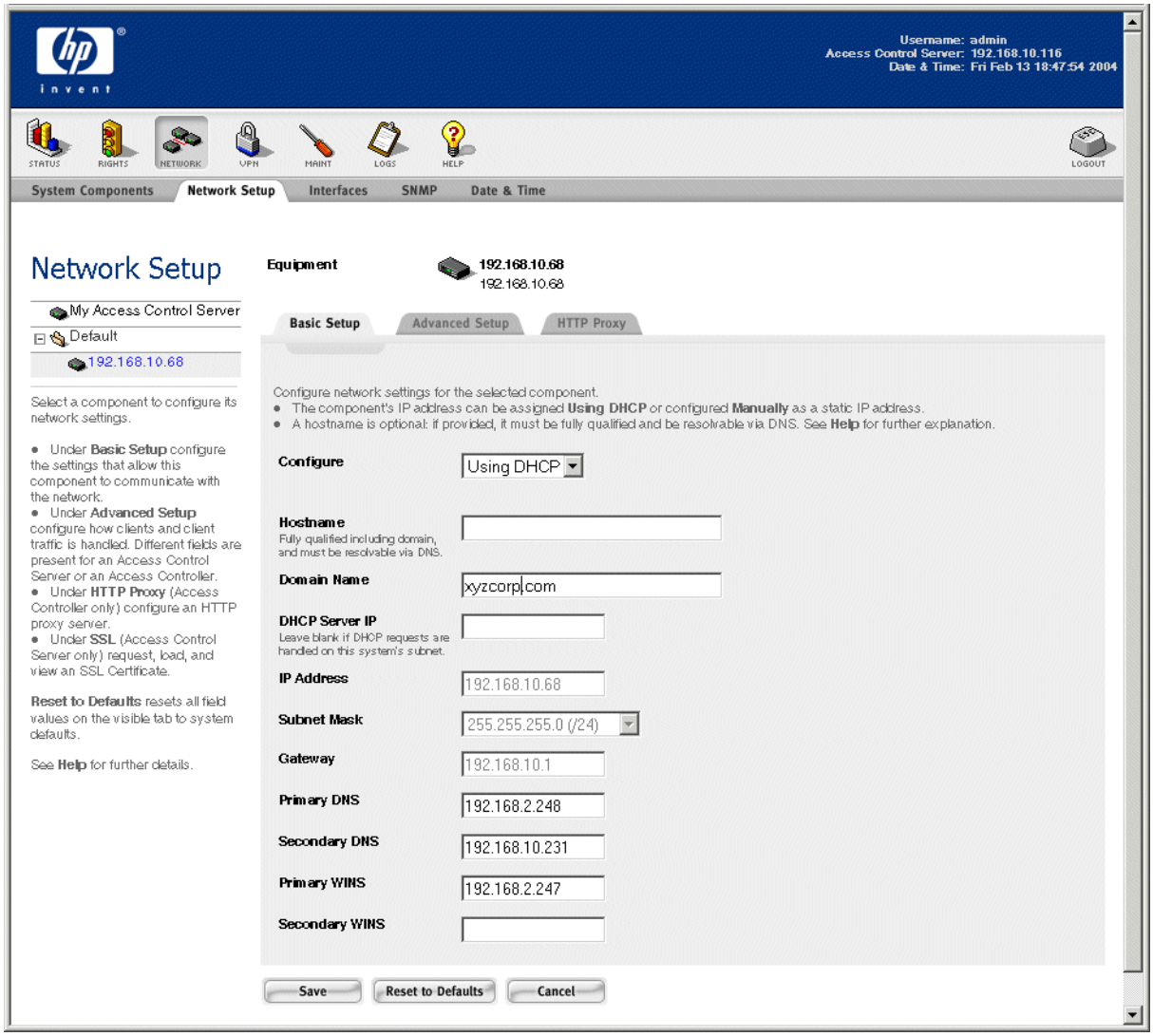
a. Click the **NETWORK** button. The System Components page appears, as shown in Figure 3-13.

Figure 3-13. System Components page



b. Click the **Network Setup** tab just below the row of function buttons. This brings up the Network Setup page (see Figure 3-14).

Figure 3-14. Network Setup page



c. From the System Components List under in the left panel (under the Network Setup heading) select the Access Controller you just installed to display its **Basic Setup** page.

d. Verify that the information for the Access Controller is correct, or enter additional settings as necessary. From the **Advanced Settings** sub-tab you can configure Bridging, IP broadcast forwarding, and client polling; from the **HTTP Proxy** sub-tab you can configure the address of a proxy server for HTTP requests.

e. Click **Save** to save any changes you have made to any of the sub-tabs on this page.

f. Click the **Date & Time** tab to display the Date & Time page, then again select the Access Controller from the System Components List.

g. To set the time zone, select the appropriate setting from the drop-down list.

h. To configure an NTP server, click the Set time using network time server checkbox, and type the IP address of a primary and (optionally) a secondary NTP server.

i. Click **Save**.

j. To set the date and time immediately, select the appropriate values and click **Set Time Now**.

Note: *You cannot set the time zone or NTP server in the same operation occurrence as manually setting the time.*

Step 4. Complete the installation by connecting one or more wireless access points to the Access Controller downlink ports, using standard (straight-through) 10Base-T/100Base-TX Ethernet cables.

See the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for detailed information on the features of the Administrative Console.

See the next chapter, "Basic Configuration" for instructions on configuring your 700wl Series system with a demonstration user account, setting up Wireless Data Privacy using PPTP, and allowing a user to connect to the system as the demonstration user.

BASIC CONFIGURATION 4

This chapter will help you accomplish the following:

- Create a demonstration user account that can log on and be authenticated through the 700wl Series system built-in user database
- Configure the 700wl Series system as a VPN gateway using PPTP encryption
- Configure a Windows client system to establish a network connection using the PPTP protocol
- Connect to the 700wl Series system as a client using the PPTP protocol, and authenticate the demonstration user against the built-in database
- (Optional) Configure the 700wl Series system to use a RADIUS server for user authentication, and log on a user that can be authenticated by the RADIUS server.

This chapter includes the following sections:

Procedure Overview

This chapter assumes that you have installed an Access Control Server and an Access Controller, or a single Integrated Access Manager, and have performed the basic configuration following the instructions in the previous chapters. It assumes you have verified that the Access Controller appears in the Access Control Server's Administrative Console.

To accomplish the objectives listed above, the instructions in this chapter lead you through the following steps:

Step 1. Create a demonstration user account (username and password) in the Rights Manager's Built-in database.

Step 2. Directly connect a Windows client system to the 700wl Series system through a downlink port of the Access Controller 720wl (or Integrated Access Manager 760wl).

Step 3. Log the user on using the default browser-based logon page.

The user should have full IP access to the network. This shows that the user can successfully connect to the system and gain network access.

Step 4. Configure the 700wl Series system to act as a VPN gateway using PPTP encryption.

Step 5. Configure the Windows client to establish a PPTP connection with the 700wl Series system.

Step 6. Connect the client to the 700wl Series system using the PPTP connection process.

The user should have full IP access to the network. Again this shows that the client can connect to the system and gain access to the network.

Step 7. (Optional) Configure the 700wl Series system to use a RADIUS server for user authentication.

Step 8. (Optional) Verify that the RADIUS Authentication Service is set up correctly using the **Trace Transaction** feature.

Step 9. (Optional) Log on using a user account known to the RADIUS authentication server, and verify network access.

The following procedures can be performed using either an Access Control Server 740wl and an Access Controller 720wl, or using a single Integrated Access Manager 760wl. The instructions are written as if an Access Control Server and a separate Access Controller are being used. If you are using an Integrated Access Manager, you perform the steps for both the Access Control Server and Access Controller on the same physical unit.

Preparation

Before you begin the system configuration process, review the following list to make sure you have the required components available and/or configured as specified:

- A management workstation running the Windows IE 6 or Netscape 7.1 browser, to be used to perform configuration tasks on the 700wl Series system.
- One Windows-based PC or Laptop preset to obtain an IP address automatically (via DHCP). This system will be used to function as a client once the configuration is complete.
- One standard (straight-through) Ethernet cable to connect the PC/laptop to a downlink port on the Access Controller or Integrated Access Manager.
- (Optional) One RADIUS Server. You must configure the RADIUS server to accept authentication requests from the Access Control Server 740wl, which acts as a RADIUS client. A user account must be created in the RADIUS database. Please consult the online Help or the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for more information on other supported external authentication servers.

Note: *If you want to use the same PC or laptop as both the management station and a demonstration client, you will need to alternately connect it either to the network (for use as a management station) or to a downlink port on the Access Controller or Integrated Access Manager (for use as a client). You will also need to force a renewal of your IP configuration each time you move from one connection to the other.*

Creating a User Account in the Built-In Database

In order for a user to log in, the 700wl Series system must be able to authenticate the user through some authentication service. The simplest form of authentication service is the built-in database included in the 700wl Series system Rights Manager. In this step, you add a user to the built-in database so you can logon to your network as that user through the 700wl Series system.

Step 1. Point your browser to the IP address or hostname of your Access Control Server or Integrated Access Manager, and log on to the Administrative Console.

Step 2. From the initial page, click on the **RIGHTS** icon () to go to the Rights Manager.

Step 3. The Rights Setup page appears.

Step 4. Click the **Identity Profiles** tab at the top of the page.

The Identity Profiles page appears, showing a list of the currently-defined Identity Profiles.

Step 5. Click the **Users** link in the left panel of the page.

The Users page appears, with an empty Users list.

Step 6. Click the **New User …** button.

The New User page appears.

Step 7. Enter the following information:

- **Name:** A descriptive name, such as "Demonstration User." This is **not** the logon name.
- **Username/MAC Address**: "demouser" (or any username you like). This is the logon name. Do **not** check the MAC Address User check box.
- **Password**: "password" (or any password you like)
  Confirm Password: must be the same as that entered into the first password field.

Step 8. Click **Save**.□

User Authentication Through the Default Logon Page

In this step, you connect your Windows PC to an Access Controller or Integrated Access Manager downlink port and log onto your network using the username and password you added to the built-in database. If this is successful, you should be able to access the Internet and other resources on your network as normal.

Note: *If you are using the same Windows PC as a client that you have been using for configuration, and the PC's network interface is configured to use a static IP address, you must change its properties so that it will obtain an IP address automatically using DHCP.*

Step 1. Plug the Ethernet cable from your PC into one of Access Controller 720wl (or Integrated Access Manager 760wl) downlink ports.

If you are using the same PC as both a client and a management station, you must release the existing IP configuration (in Windows) from the network interface of the PC as follows:

From the Windows **Start** menu, click **Run…** then enter the command `ipconfig /release`

Step 2. Power on the PC to obtain a new IP configuration from DHCP through the Access Controller 720wl, or do the following:

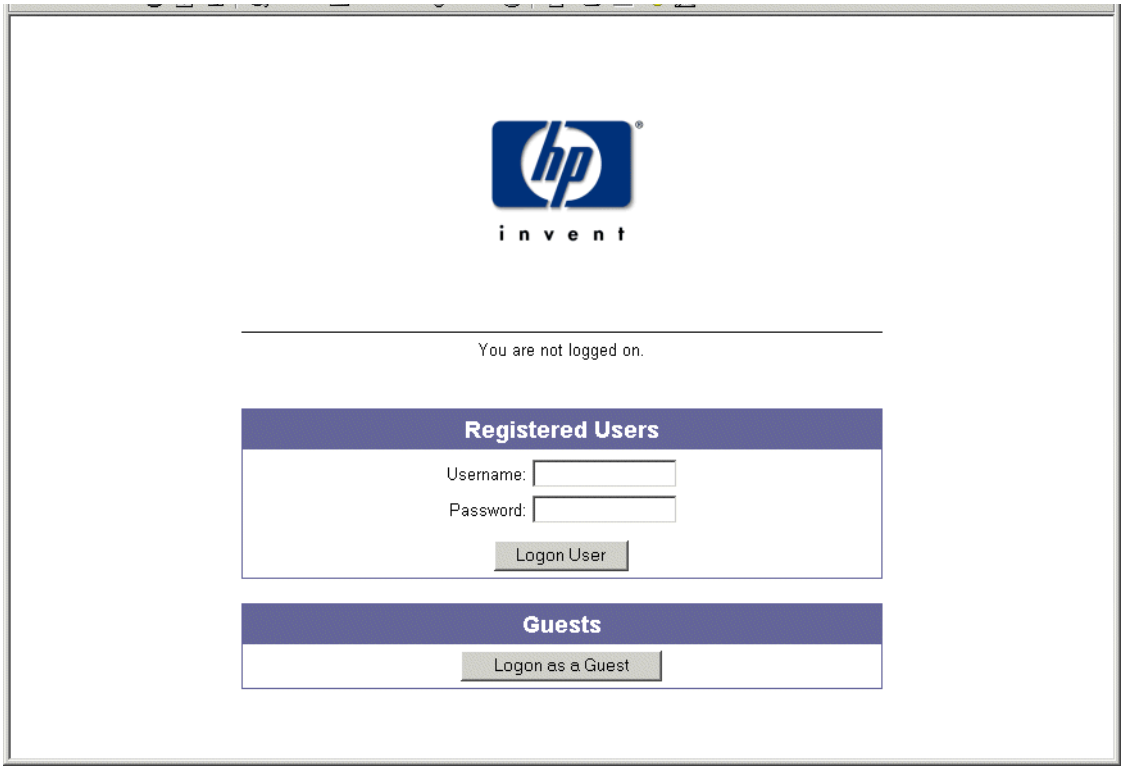
From the **Start** menu, click **Run…** then enter the command `ipconfig /renew`

The PC should receive an IP address in the 42.x.x.x range.

Step 3. Start your web browser and go to any web site. After a moment the web browser will display the HP ProCurve 700wl Series Logon page (Figure 4-1).

Note: *The 700wl Series system comes with a self-signed SSL certificate. As a result, the client browser may display a security alert warning that the certificate is not from a trusted source. Click* ***Yes*** *to proceed.*

Figure 4-1. The HP ProCurve 700wl Series user logon page



Step 4. Enter "demouser" and "password" (or the username and password you created) in the Username and Password fields and click **Logon User**.

At this point, the web page you requested should appear, and you should be able to access the network normally.

To prepare for logging on again using the PPTP connection interface, log the client off the 700wl Series system:

Step 5. Set your web browser to the URL `http://1.1.1.1`. The HP ProCurve Logon window appears, showing the user as logged on, and displaying a **Logoff** button at the top right of the window.

Step 6. Click the **Logoff** button to log the client off the system.

PPTP Gateway Configuration

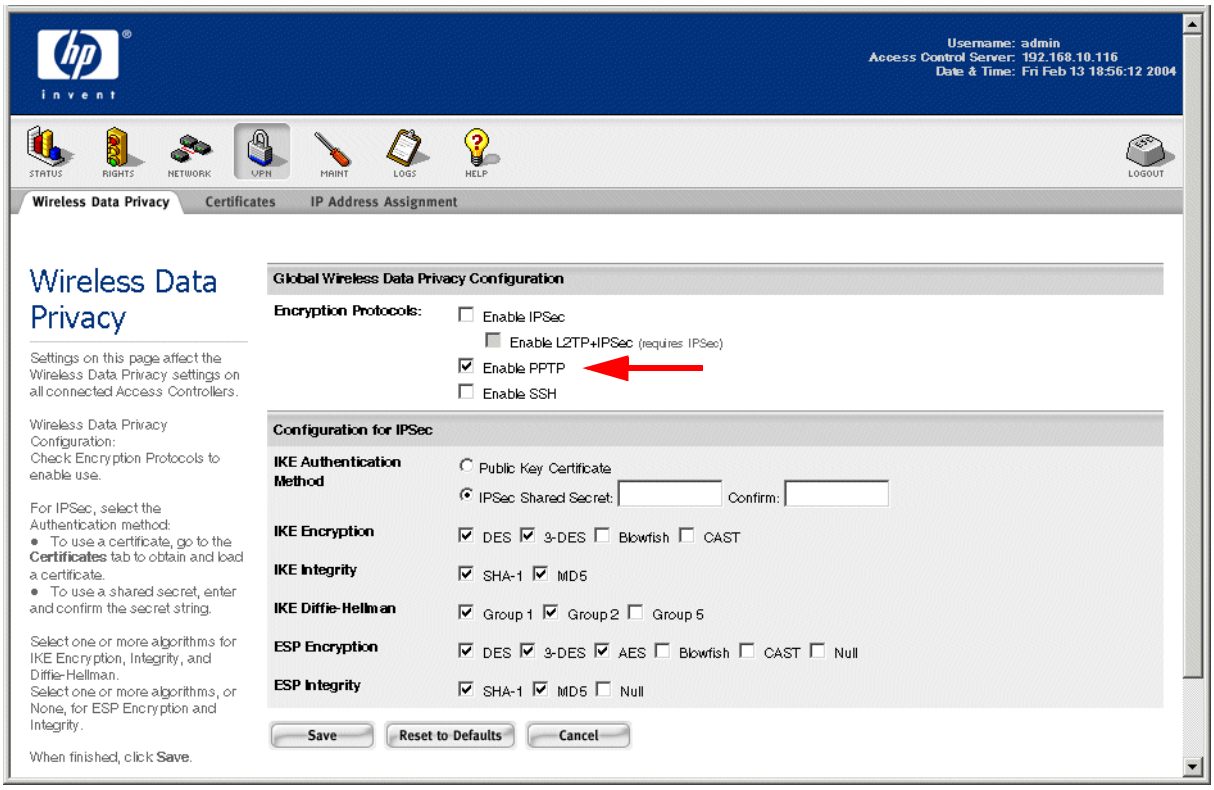
This step configures the 700wl Series system to act as a VPN termination for PPTP. After configuring the PPTP client on your PC (see "PPTP Client Configuration" on page 4-8), you should be able to logon to the network via the PPTP connection interface.

The steps below have you change the setting for the default Authenticated Access Policy so that it uses PPTP. Optionally, you can set up a new Access Policy to use PPTP. See the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for further details, if needed.

Step 1. From your management station, point your browser to the IP address or hostname of your Access Control Server or Integrated Access Manager, and logon to the Administrative Console. The initial page of the Administrative Console appears.

Step 2. Click the **VPN** button to go to the Wireless Data Privacy configuration page (see Figure 4-2).

Figure 4-2. Enabling PPTP for the 700wl Series system



Step 3. Under **Encryption Protocols**, put a check mark in the **Enable PPTP** checkbox, then click **Save**.

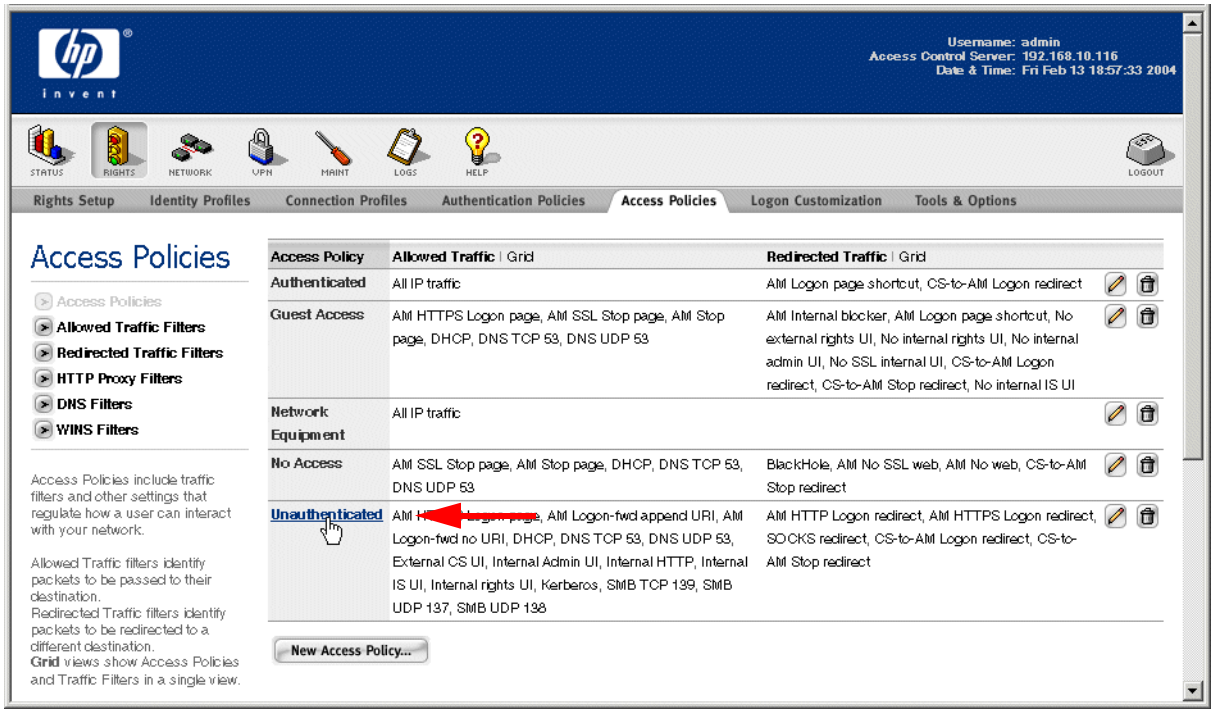
Configuring Access Policies for Encryption

The next step is to configure the appropriate Access Policies to allow the use of encryption. You must allow encryption for the "Unauthenticated" Access Policy so that an unknown client using encryption can connect to the 700wl Series system, and you must enable encryption for the relevant Access Policy that will take effect once the client has been successfully authenticated—in this case, the "Authenticated" Access Policy.

Step 1. From the Navigation toolbar, click the **RIGHTS** button ( ) to go to the Rights Manager.

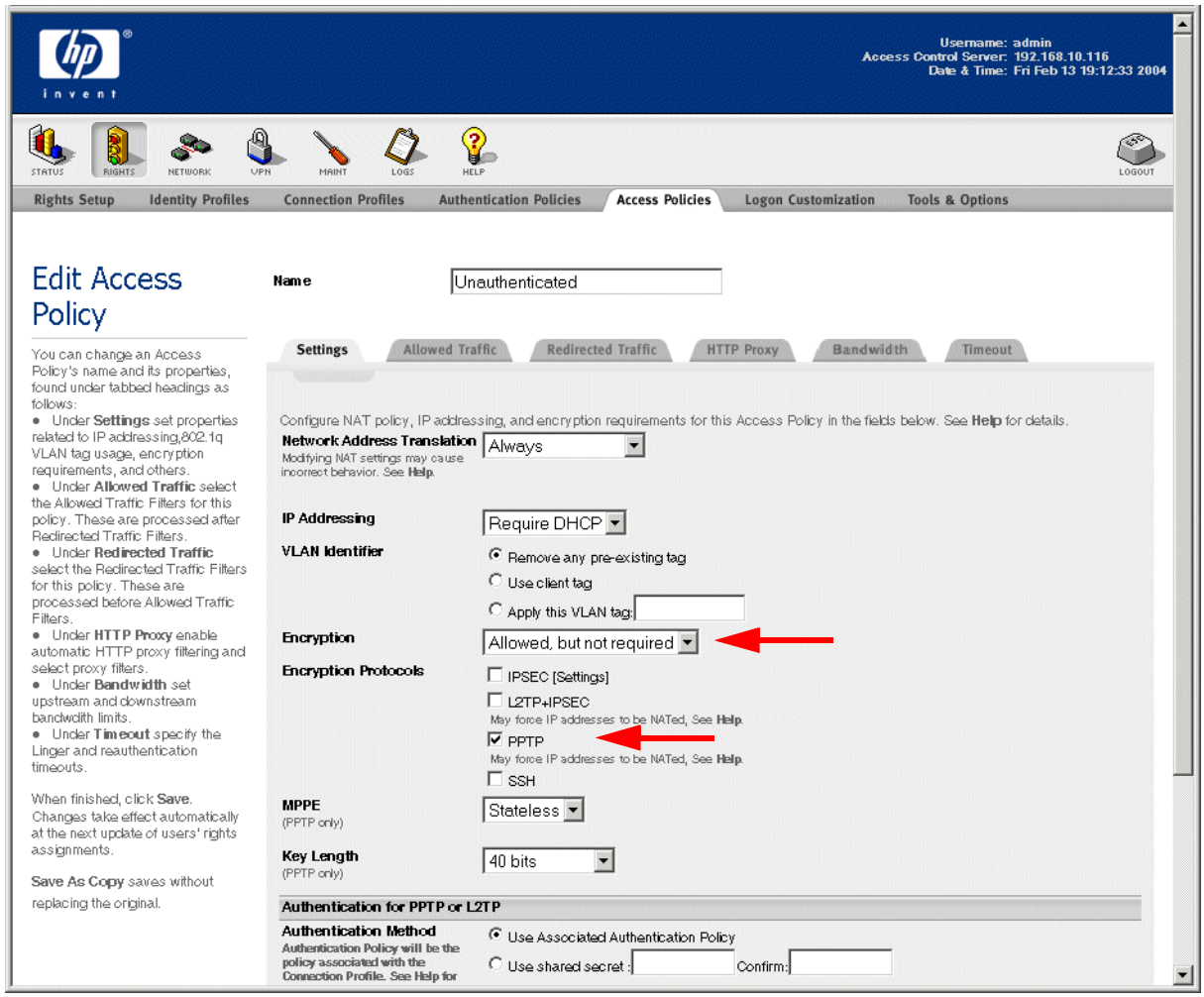
Step 2. Click the **Access Policy** tab to go to the Access Policies page, as shown in Figure 4-3.

Figure 4-3. Access Policies page



Step 3. Click on the name **Unauthenticated** in the list of Access Policies to bring up the Edit Access Policy page for the Authenticated Access Policy. See Figure 4-4.

Figure 4-4. Edit Unauthenticated Access Policy page



Step 4. Select "Allowed, but not required" from the drop down menu for Encryption.

Step 5. Under **Encryption Protocols**, put a check mark in the **PPTP** checkbox. Leave the other settings as they are.

Step 6. Click **Save** to save your changes to the "Unauthenticated" Access Policy.

Step 7. Return to the Access Policies page, select the "Authenticated" Access Policy (at the top of the Access Policies list) and make the same changes (Steps 4 through 7).

Now users will be able to log on either using PPTP or without using encryption. In order to use PPTP, the client must be configured to use PPTP, as described in the following section.

PPTP Client Configuration

This next set of steps configures the PPTP client on the Windows PC. These instructions are for Windows XP, but the process is similar for Windows 2000.

Step 1. Open the Network Connections window:

- Click the **Start** button and select **Control Panel**.
- From the Control Panel window, double-click **Network Connections**.

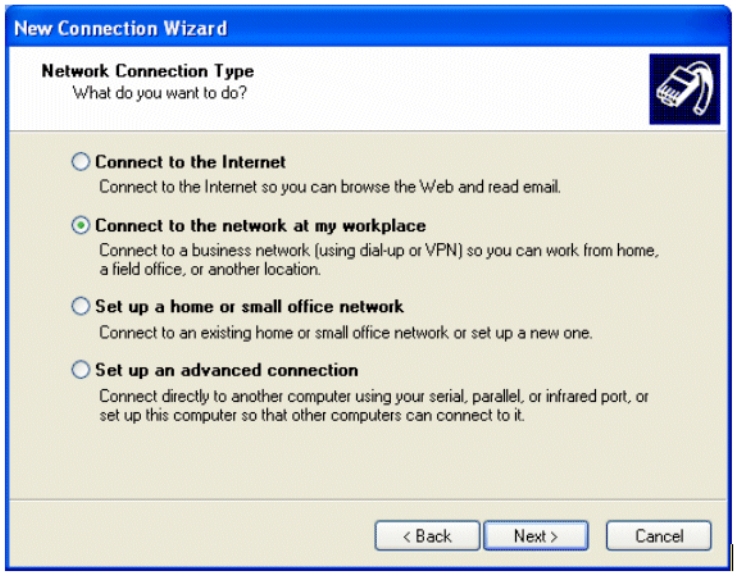
The Network Connections window appears.

Step 2. Click on the **New Connection Wizard** link on the Network Connections window.

The New Connection Wizard window appears.

Step 3. Click **Next>** to go to the Network Connection Type page.

Figure 4-5. Connection Wizard Window—Network Connection Type Page



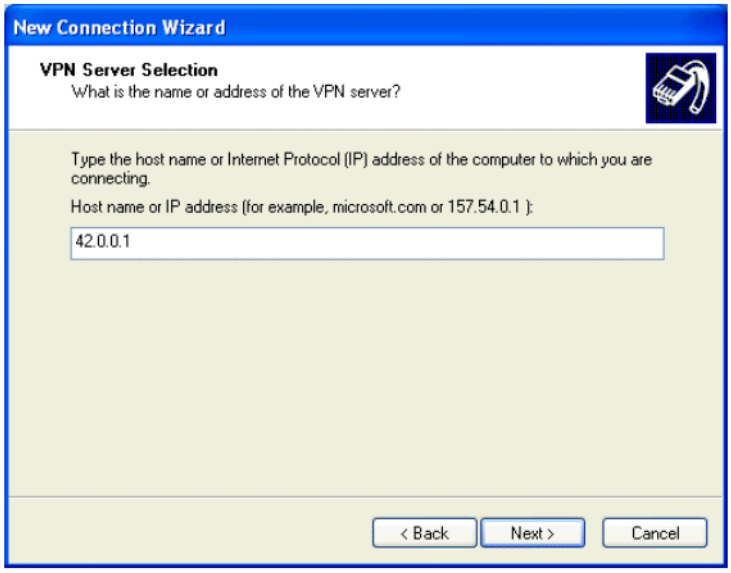
Step 4. Select the **Connect to the network at my workplace** option and then click **Next >**.

Step 5. Select the **Virtual Private Network** connection option. Click **Next >**.

Step 6. Enter the desired connection name in the **Company Name** text box and then click **Next >**.

Step 7. You should now be at the VPN Server Selection page. Enter `42.0.0.1` in the **Host name or IP address** text box and then click **Next >**.

Figure 4-6. Connection Wizard Window—VPN Server Selection



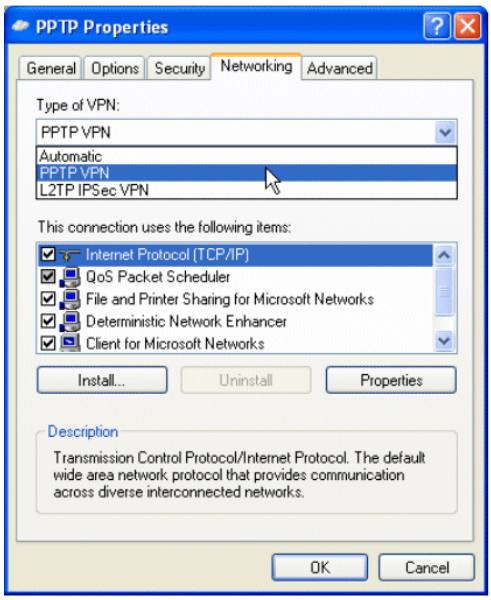
Step 8. The Completing the New Connection Wizard page appears. You may choose to add a shortcut to this connection to the desktop, then click Finish

An icon representing the new connection appears in the Network Connections window under the Virtual Private Network section. In addition, the Sign-on window should appear on the screen; if it does not, double-click the new connection icon.

Figure 4-7. Connection Sign-On Window

Step 9. Click the **Properties** button to open the connection's properties window.

Figure 4-8. Connection Window—PPTP Properties



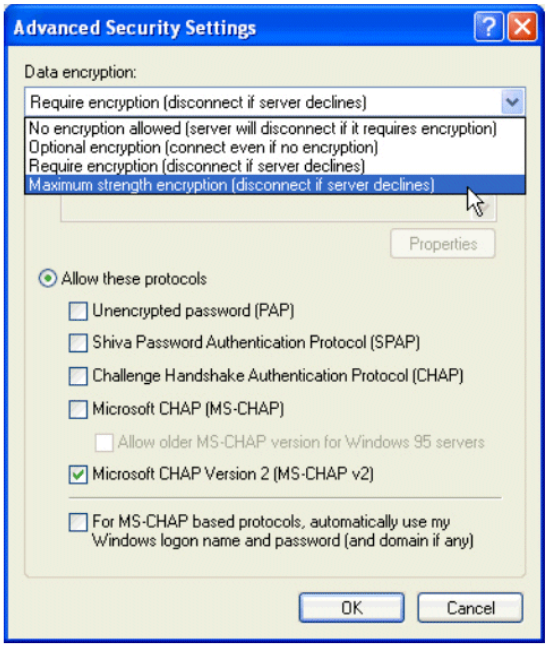
Step 10. Click the **Networking** tab to specify the type of VPN.

Step 11. Select **PPTP VPN** from the drop-down menu for **Type of VPN**.
Make sure that Internet Protocol (TCP/IP) is selected.

Step 12. Click the **Security** tab to customize the security protocols.

Step 13. Select **Advanced (custom settings)** on the Security page and click the **Settings** button. The Advanced Security Settings window appears. See Figure 4-9

Figure 4-9. Connection Window—Advanced Security Settings



Step 14. Deselect the Microsoft CHAP (MS-CHAP) protocol option (this protocol is selected by default). Leave Microsoft CHAP Version 2 selected. Only MS-CHAP v2 is set for use with the Authenticated Access Policy.

Step 15. Select **Maximum strength encryption (disconnect if server declines)** from the drop-down menu for **Data Encryption**. This sets the length of the encryption key to 128 bits.

Step 16. Click **OK** to go back to the connection's properties window.

Step 17. Click **OK** to go back to the Connect window.

Step 18. Click **Cancel** to close the Connect window.

User Authentication Via PPTP Connection

Before starting the VPN connection, make sure your system has established a network connection with the Access Control Server. You can use the `ipconfig` command to verify the IP settings or use the `ipconfig /renew` command to obtain an IP configuration from the Access Control Server 740wl.

Step 1. Open the PPTP connection created by the procedure specified above in the section "PPTP Client Configuration" on page 4-8. Use the shortcut on your desktop or open the connection from the Network Connections window in the Control Panel.

The Connect window appears.

Step 2. Type "demouser" and "password" (or the user name and password you created in the built-in database) in the **Username** and **Password** field, and click **Connect** to connect to the server.

You may choose to save this username and password for future use before clicking the Connect button.

After the connection is successfully made, the connection icon appears in the notification area on the lower-right corner of the screen as shown below.

Figure 4-10. Connection icon

External Authentication Service Configuration (Optional)

If you use an external RADIUS authentication service and your user account already exists in the RADIUS server's database, you can configure the 700wl Series system to authenticate using the RADIUS server rather than the built-in database.

Once you have successfully completed this configuration, you should be able to logon to the network through the 700wl Series system using any legitimate username and password recognized by your RADIUS server.

Note: *Your RADIUS server must be configured to recognize the Access Control Server as a RADIUS client.*

To configure the Rights Manager to use a RADIUS server for authentication, do the following:

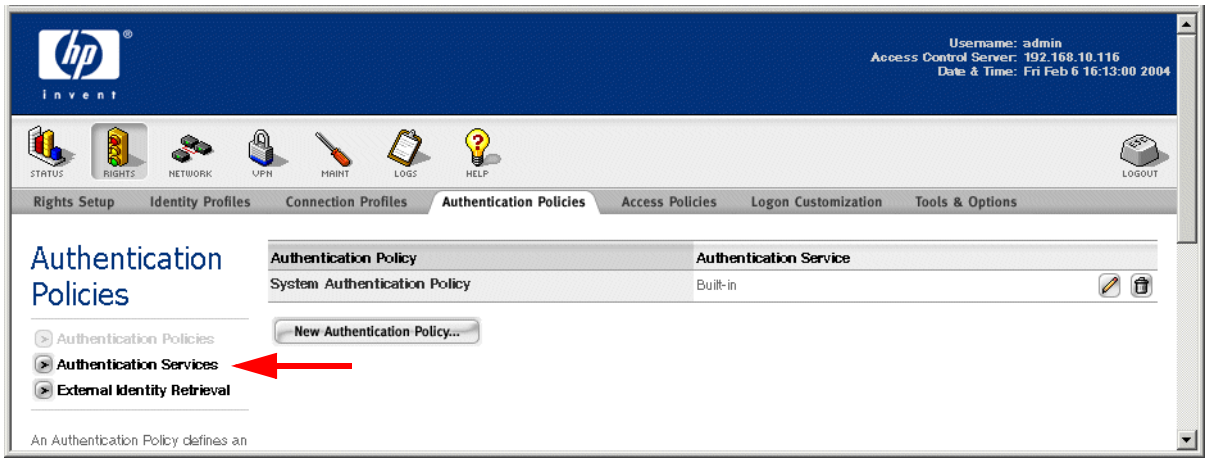
Step 1. From your management station, point your browser to the IP address or hostname of your Access Control Server or Integrated Access Manager, and logon to the Administrative Console.

The initial page of the Administrative Console appears.

Step 2. Click the **RIGHTS** icon ( ) to go to the Rights Manager.

Step 3. Click the **Authentication Policies** tab to go to the Authentication Policies page (see Figure 4-11).

Figure 4-11. Authentication Policies page

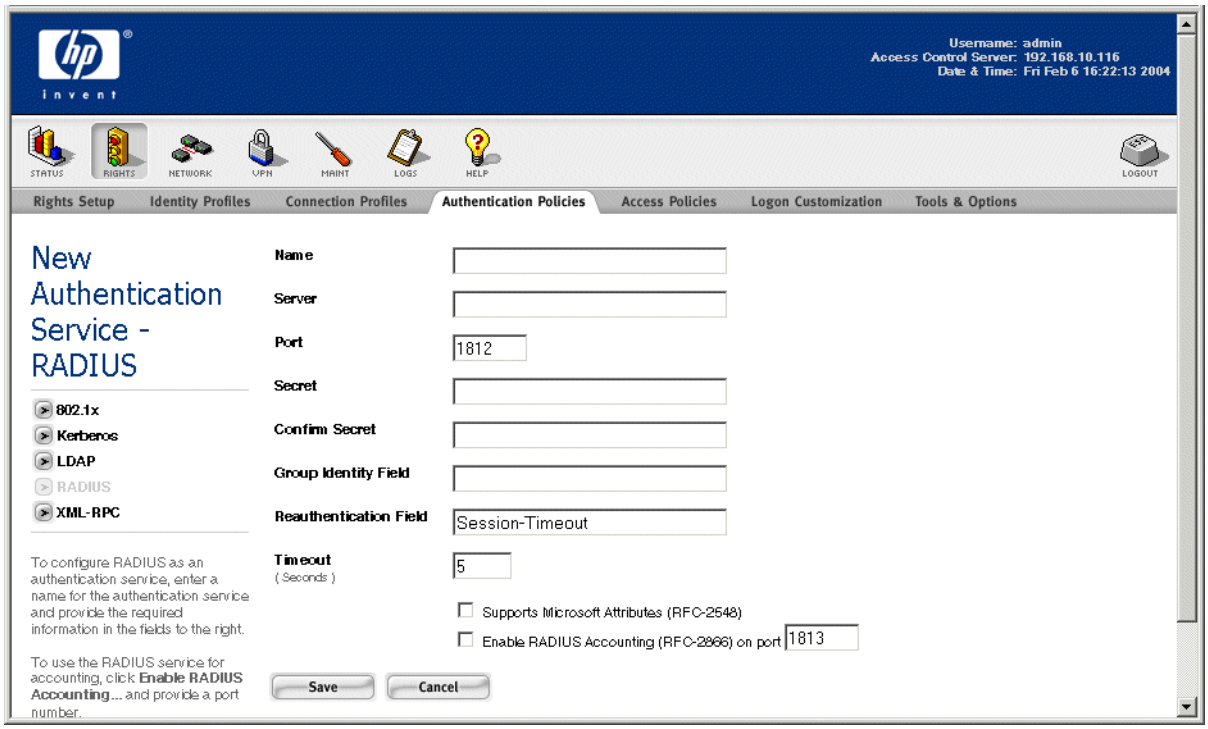


Step 4. Click the **Authentication Services** link in the left panel of the page.
The Authentication Services page appears.

Step 5. Click **New Service ...**.
The New Authentication Service — LDAP page appears.

Step 6. Click the **RADIUS** link in the left pane of the page.
The New Authentication Service — RADIUS page appears, as shown in Figure 4-12.

Figure 4-12. Configuring a RADIUS Authentication Service



Step 7. Type the required information into the appropriate fields.

- Enter a name for this authentication service in the **Name** field.
- Enter the **Server** and **Port** information for your RADIUS server.
- Enter the **Secret** that matches the secret configured on your RADIUS server, and enter it a second time as a confirmation.
- Leave the **Group Identity Field** blank. This field is used to specify the name of a RADIUS attribute that contains group information used to assign the authenticated user to an Identity Profile.

  If you elect to use this field, you must also create an Identity Profile to match the group name that will be returned, and then add a row to the Rights Assignment Table to associate an Access Policy with that Identity Profile.
- You can leave the default attribute name for the **Re-authentication Field**. This field specifies the name of a RADIUS attribute that specifies the duration (in seconds) after which the client is forced to reauthenticate.
- Enter the authentication time-out period (in seconds) in the **Timeout** field, or leave the default.

Step 8. Click **Save**.

The Authentication Services page will reappear.

Step 9. Click the **Authentication Policies** link in the left panel of the page.

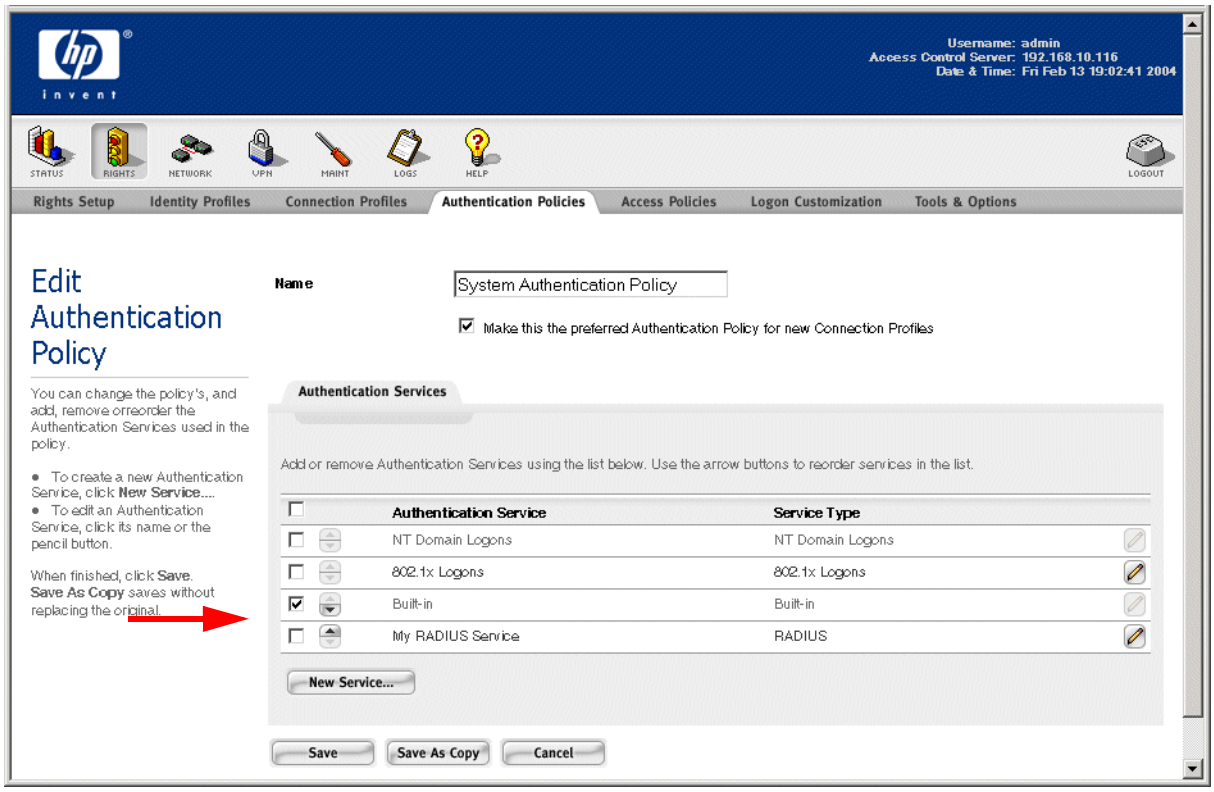
The Authentication Policies page will appear.

Step 10. Click the **System Authentication Policy** name in the table of Authentication Policies.

Step 11. The Edit Authentication Policy page appears (see Figure 4-13).

The newly added authentication service appears at the bottom of the list of available Authentication Services for this Authentication Policy.

Figure 4-13. Editing the System Authentication Policy



Step 12. Use the row up/down buttons to move the newly added RADIUS authentication service ahead of the Built-in service, and put a check next to this service. (Leave the Built-in service checked as well.)

Step 13. Click **Save**.

The new RADIUS authentication service will now be the initial service used to authenticate user who are being authenticated by the System Authentication Policy. The System Authentication Policy is used by the default Connection Profile "Any."

Note: *After you complete this step you will still be able to log in using the "demouser" username, because the built-in database will still be searched if the user was not authenticated by the RADIUS server.*

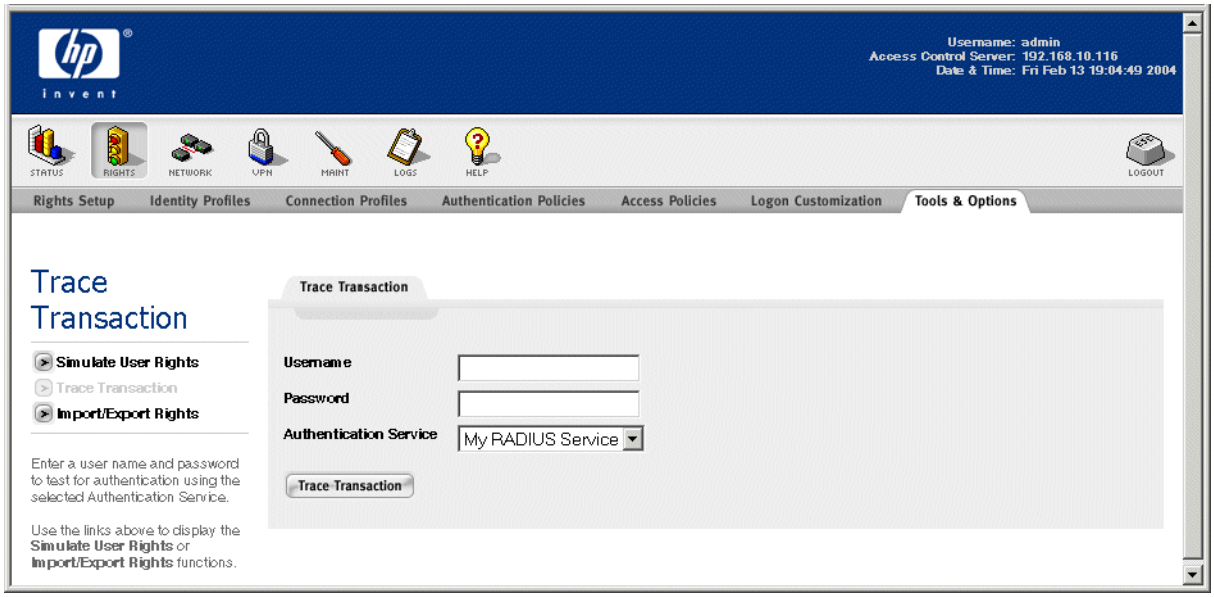
Verify the External Authentication Service

The following steps allow you to verify that your RADIUS server will correctly authenticate users:

Step 1. Click the **RIGHTS** icon ( ) to go to the Rights Manager.

Step 2. Click the **Tools & Options** tab, then click the **Trace Transaction** link in the left panel. The Trace Transaction page appears, as shown in Figure 4-14.

Figure 4-14. Trace Transaction page



Step 3. Enter a known user name and password into the **Username** and **Password** fields

Step 4. Make sure the RADIUS authentication service you created is selected in the Authentication Service drop-down list and click **Trace Transaction**.

This function displays both the information sent to the Authentication Service and the returned results. If something is incorrect, the Results Parameters will indicate an error. Possible reasons for the error include:

- Invalid Username or Password or both
- The RADIUS authentication service is not configured correctly
- The RADIUS Server does not recognize the Access Control Server 740wl

If an error occurs, return to "External Authentication Service Configuration (Optional)" on page 4-11 and verify the RADIUS server configuration. Make sure to use a legitimate username and password recognized by the RADIUS server to test the RADIUS server.

If the RADIUS service works correctly, you should now be able to log off the "demouser" user (by going to URL `http://1.1.1.1`) and log on again as a valid RADIUS user.

TROUBLESHOOTING

A

This chapter presents troubleshooting procedures for the 700wl Series. Table A-1 shows the symptoms, probable cause and recommended action for a non-responsive unit.

Table A-1. Troubleshooting Guide

Symptom(s)	Probable Cause	Recommended Action
Power LED Off	No Power	Check power cord and AC outlet
Power LED on but fans not running	Defective Fan	Replace Fan
Unit inaccessible from customer network after configuration	Incorrect Cabling	1. Use straight-through Ethernet Cable. 2. Ensure connectivity to network
Unit inaccessible from management system after configuration	Incorrect configuration	Access system through network uplink, check configuration. Check in particular that IP address and hostname are correct, and that hostname agrees with IP address.
	Incorrect network configuration	1. Check default router. 2. Check DNS server configuration 3. Check subnet mask 4. Check configuration of unit to use DHCP or static ip address.
	If all else fails	1. Reboot using command line interface. 2. Restart management system 3. Restore to factory defaults and start over
Can't get to Access Control Server Administrative Consoler	Incorrect password	1. Check configuration, particularly passwords 2. Use CLI to reset passwords

Table A-1. Troubleshooting Guide (Continued)

Symptom(s)	Probable Cause	Recommended Action
No traffic through access point	No connection	1. Check cabling to access point. 2. Use cross-over cable if required 3. Check power to Access Point
	Access point requires server for WEP Key	Create Identity Profile for MAC address of access point that allows this traffic for each access point.
	Access Point requires configuration	If Access point uses static IP or wants a dynamic IP address from network DHCP server, make sure 700wl Series system system is not doing NAT for Access Point (create Identity Profile for MAC address of Access Point that allows Real IP Mode)
No initial web page	Access Controller sees no web request	Use a browser to request http://1.1.1.1
	Browser problems	Internet Explorer 5.01 with DLL schannel.dll version 4.86.1959.1877 is known to have broken SSL
		Certain downrev versions of MAC OS/X browsers have broken SSL

LCD DISPLAY DESCRIPTION

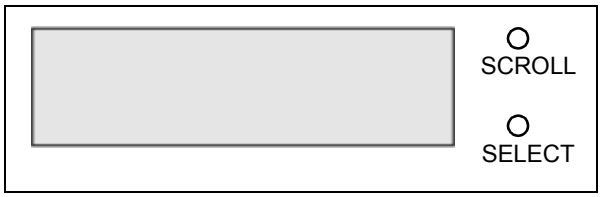
B

This appendix describes the LCD display on the Access Controller 720wl, Access Control Server 740wl, and Integrated Access Manager 760wl. The display can be used to view the system's network parameters, and to power down the system. This appendix contains the following sections:

Display Description

The LCD display is located in the middle of the front panel of 700wl Series Products. It is a 16 character by two line display, with two buttons located to the right of the display (Figure B-1).

Figure B-1. LCD Display



The top button is labeled *SCROLL*. Pressing the *SCROLL* button cycles through the various displays. The bottom button is labeled *SELECT*. Pressing the *SELECT* button causes whatever action is currently on the display to be taken.

Note: *An unusual voltage surge including static discharge can cause the LCD on the front of the unit to become incorrect and unresponsive. To correct this situation, the unit must be restarted (power cycled).*

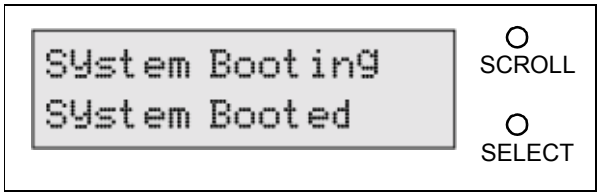
Powering On and System Boot

At power-on, the display remains blank until the system has initialized itself and displays *System Booting* (Figure B-2).

Figure B-2. System Booting

When the booting is finished, the *System Booted* display appears (Figure B-3).

Figure B-3. System Booted

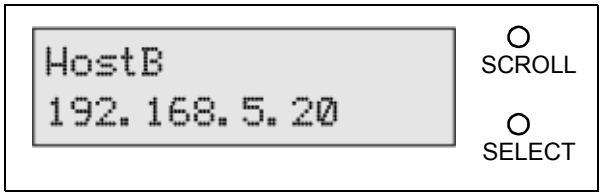


The system then goes to the default display within a few seconds.

Default Display

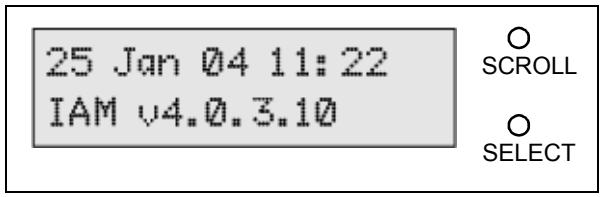
Once the system has finished booting, the LCD will alternate between the Hostname/IP Address Display (Figure B-4), and the Date Time/Version Display (Figure B-5).

Figure B-4. Hostname/IP Address Display



The Hostname/IP Address display shows the hostname (if set, and not fully-qualified) and IP Address of the unit.

Figure B-5. Date Time/Version Display



The Date Time/Version Display shows the date and time, and the version number of the software installed on the system. The indicator shows whether the unit is an Access Controller(AC), Integrated Access Manager (IAM) or Access Control Server (ACS).

Each display shows for approximately 10 seconds. The system returns to this default display automatically, regardless of the current display, if no buttons are pressed for approximately 30 seconds.

Software Download and Upgrade

When you initiate the download of a new software image, the display indicates the progress of the download as shown in Figure B-6. This shows the number of Megabytes received compared to the number of Megabytes in the load number (in the example, 72.8 MB). This is updated every few seconds.

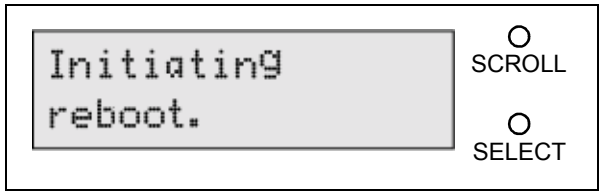
Figure B-6. Software download progress display

Once the full load has been received, the display indicates that the image is being installed as the alternate image (Figure B-7).

Figure B-7. New image installation display

Once the image is installed, if you have requested an immediate reboot with the new image, the display indicates when the reboot is initiated, as shown in Figure B-8.

Figure B-8.



Main Menu

When the default display (either the Hostname/IP Address or the Date Time/Version) is showing, repeatedly pressing the *SCROLL* button will cycle through the Main Menu items. These are:

- Main Menu (Figure B-9)
- Network Config (Figure B-10)
- System Shutdown (Figure B-11)

If you press both the *SCROLL* and *SELECT* buttons at the same time, from any other display, you will also see the Main Menu.

Figure B-9. Main Menu Display

Figure B-10. Network Configuration Display

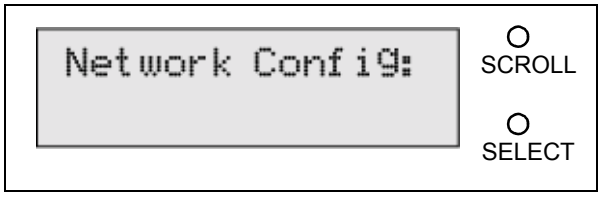
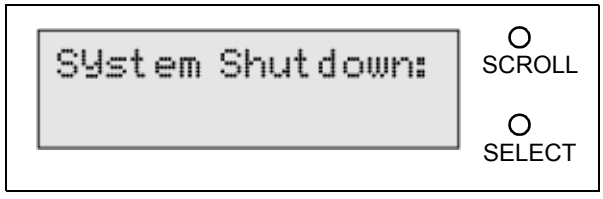


Figure B-11. System Shutdown Display



Network Configuration

If you press the *SELECT* button while *Network Config* is displayed, you enter the Network Configuration sub-menu. Repeatedly pressing the *SCROLL* button will cycle through the Network Configuration sub-menu items. These are:

- IP Address (Figure B-12)
- Subnet Mask (Figure B-13)
- Default Router (Figure B-14)
- Primary DNS (Figure B-15)
- Secondary DNS (Figure B-16)
- <Previous Menu (Figure B-17)

Figure B-12. IP Address Display

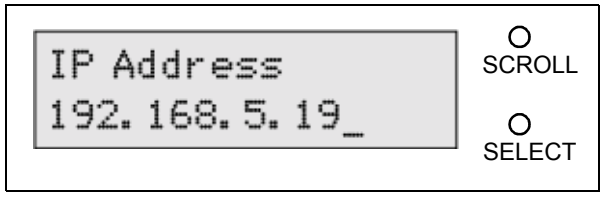


Figure B-13. Subnet Mask Display

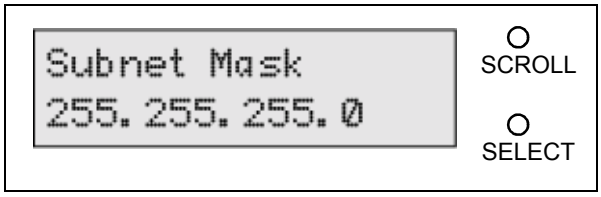


Figure B-14. Default Router Display

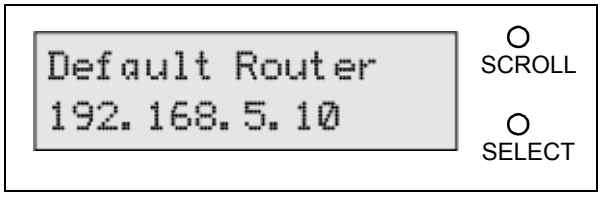


Figure B-15. Primary DNS Display

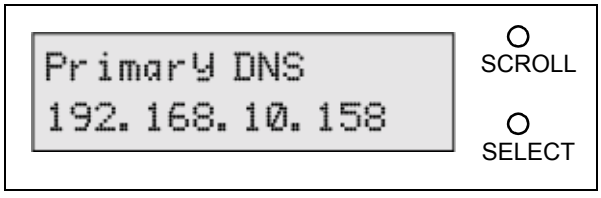


Figure B-16. Secondary DNS Display

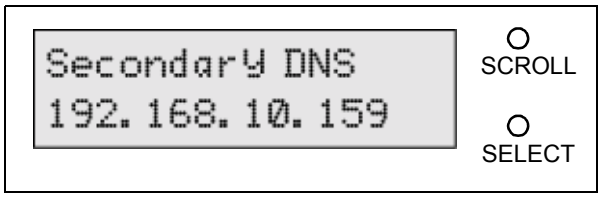
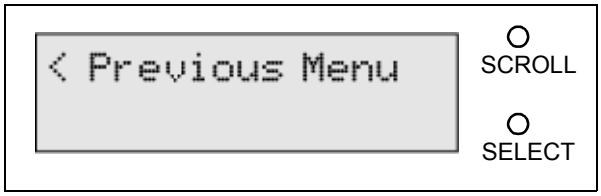


Figure B-17. Previous Menu Display

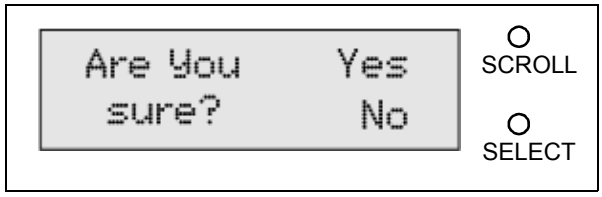


Pressing the *SELECT* button while *<Previous Menu* is displayed will always return you to the previous menu.

System Shutdown

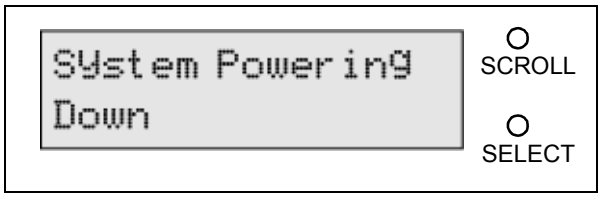
Pressing the *SELECT* button while *System Shutdown* is displayed allows you to shutdown and power off the system. After pressing the *SELECT* button, *Are You Sure?* displays (Figure B-18):

Figure B-18. Are You Sure Display



If you are sure you want to shutdown and power off the system, press the *SCROLL* button. Otherwise, press the *SELECT* button, and the display returns to the Main Menu item *System Shutdown*. If you choose to shutdown the system, the *System Powering Down* display appears (Figure B-19).

Figure B-19. System Powering Down



A system can take up to 30 seconds to perform the shutdown and power-off sequence.

C

TECHNICAL SPECIFICATIONS, SAFETY AND COMPLIANCE

This appendix describes the technical specifications for the HP ProCurve 700wl Series.

Technical Specifications

Environmental Ranges

Operating Temperature Range, °C	0 to +40
Storage Temperature Range, °C	-25 to +70
Humidity Range, non-condensing, percent	5 to 90
Operating Altitude	Up to 10,000 ft (3000 m)
Storage Altitude	Up to 15,000 ft (4570 m)

Power Requirements

	6500 Series	**6500p Series**
AC Voltage	100-240 VAC	100-240 VAC
Power Supply Rating	6A @ 110VAC 3A @ 240VAC	6A @ 110VAC 3A @ 240VAC
Frequency Range	50 or 60 Hz	50 or 60 Hz
Heat Dissipation (BTU/Hr.)	170 BTU/Hr	170 BTU/Hr
Power Consumption (Max)	2.5A	5A
Power Consumption (Nominal)	1.5A	3.5A
Per Port Power Rating	N/A	315ma@48VDC

Physical Dimensions

Weight	20 lbs (9 kg)
Height	3.5 in. (8.9 cm)
Width	17.0 in. 43.2 cm)
Depth	15.0 in. (38.1 cm)

Safety and Regulatory Compliance

Safety Standards

UL 60950
EN 60950:2000
CAN/CSA 22.2 No. 60950

EMC Compliance

FCC Part 15 Class A
EN 55022 (1998) Class A
EN 55024 (1998)
VCCI Class A
EN61000-3-2 (1995) w/A1 & A2 (1998)
EN61000-3-3 (1995) w/A1 (1998)

Physical Interface

Network Connector	RJ45 10/100Base-T /1000Base-TX
Device Connectors	RJ45 10/100Base-T
Management Console port	DB-9, male
LEDs	Power, Link, Activity, Hard Disk
Management Display	2-line LCD

CABLE AND CONNECTOR SPECIFICATIONS D

This appendix describes the Serial Connector and the Standard Ethernet cables for use with non-powered devices. This appendix contains the following sections:

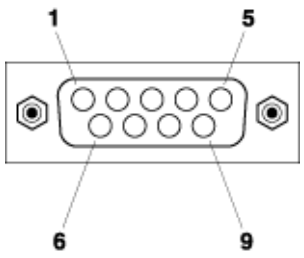
Serial Connector

Table D-1 shows the pin assignments for the serial connector, and Figure D-1 shows the pin configuration. If you are connecting a Console Device such as a laptop, you must use a serial crossover cable (null modem cable).

Table D-1. Pin assignments for serial connector

Pin	Assignment	Symbol
1	Data Carrier Detect	DCD
2	Receive Data	RXD
3	Transmit Data	TXD
4	Data Terminal Ready	DTR
5	Signal Ground	GND
6	Data Set Ready	DSR
7	Request to Send	RTS
8	Clear to Send	CTS
9	Ring Indicator	RI

Figure D-1. Serial Port pin configuration



10/100 Downlink Ethernet Connectors

Table D-2 shows the RJ45 pin numbers and functions for 10/100 Ethernet ports.

Table D-2. Pin numbers and functions for standard Ethernet cables

Pin Number	Standard Ethernet
1	Incoming Data + (RD+)
2	Incoming Data - (RD-)
3	Outgoing Data + (TD+)
4	No Connection (NC)
5	No Connection (NC)
6	Outgoing Data - (TD-)
7	No Connection (NC)
8	No Connection (NC)

Option Card Ports and Cables

Ports

- The ports on the HP ProCurve 10/100 Module are compatible with the IEEE 802.3 10Base-T and 802.3u 100Base-TX standards, and accept the 10 Mbps or 100 Mbps cables listed in Table D-3.
- The port on the HP ProCurve 10/100/1000Base-T Module is compatible with the IEEE 802.3 10Base-T, 802.3u 100Base-TX, and 802.3ab 1000Base-T standards, and accept the 10 Mbps, 100 Mbps, or 1000 Mbps cables listed in Table D-3. For 1000 Mbps operation, Category 5E shielded twisted pair cable is recommended.
- The port on the HP ProCurve Gigabit SX Module transmits at 850 nanometer wavelength, and is compatible with the IEEE 8021.3z Gigabit-SX standard. It accepts the multi-mode fiber-optic cables listed in Table D-3.
- The port on the HP ProCurve Gigabit LX Module transmits at 1310 nanometer wavelength, and is compatible with the IEEE 8021.3z Gigabit-LX standard. It accepts the single-mode or multi-mode fiber-optic cables listed in Table D-3.

Cables

The following table summarizes the characteristics of the cables you should use to connect to the option card ports on your 700wl Series system.

Table D-3. Summary of cable types for use with option cards

Port Type (Module)	Cable Type	Maximum Length
10Base-T/ 100Base-TX (HP ProCurve VXM-14 4-port 10/100 Module)	**10 Mbps operation:** Category 3, 4, or 5, 100-ohm shielded twisted pair (STP) cable complying with IEEE 802.3 10Base-T specifications, fitted with RJ-45 connectors **100 Mbps operation:** Category 5 100-ohm STP cable complying with IEEE 802.3u 100Base-TX specifications, fitted with RJ-45 connectors	100 meters
10/100/1000Base-T (HP ProCurve VXM-17 10/100/1000Base-T Module)	**10 Mbps operation:** Category 3, 4, or 5, 100-ohm shielded twisted pair (STP) cable complying with IEEE 802.3 10Base-T specifications, fitted with RJ-45 connectors **100 Mbps operation:** Category 5 100-ohm STP cable complying with IEEE 802.3u 100Base-TX specifications, fitted with RJ-45 connectors **1000 Mbps operation:** Category 5E 100-ohm 4-pair STP cable complying with IEEE 802.3ab 1000Base-T specifications, fitted with RJ-45 connectors (see Note on 1000Base-T Cable Requirements on page D-3.)	100 meters
Gigabit SX (HP ProCurve VXM-19 Gigabit-SX Module)	Gigabit Ethernet short reach, multi-mode, 850 nm transceiver, LC connector Cables with SC connectors may be used with an LC-to-SC media converter (included with card)	500 meters
Gigabit LX (HP ProCurve VXM-13 Gigabit-LX Module	Gigabit Ethernet long reach, single-mode, 1310 nm transceiver, LC connector Cables with SC connectors may be used with an LC-to-SC media converter (included with card)	5 kilometers

Note: 1000Base-T Cable Requirements. *The Category 5 networking cables that work for 100Base-TX connections should also work for 1000Base-T, as long as all four-pairs are connected. However, for the most robust connections you should use cabling that complies with the Category 5E specifications as described in Addendum 5 to the TIA-568-A standard (ANSI/TIA/EIA-568-A-5)*

SAFETY AND EMC REGULATORY STATEMENTS

E

Safety Information

Documentation reference symbol. If the product is marked with this symbol, refer to the product documentation to get more information about the product.

WARNING A WARNING in the manual denotes a hazard that can cause injury or death.

CAUTION A CAUTION in the manual denotes a hazard that can damage equipment.

Do not proceed beyond a WARNING or CAUTION notice until you have understood the hazardous conditions and have taken appropriate steps.

Grounding

These are safety class I products and have protective earthing terminals. There must be an uninterruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

Shielded Signal Cables

Use only shielded cables for connecting peripherals to any HP ProCurve 700wl Series device to reduce the possibility of interference with radio communications services. Using shielded cables ensures that you maintain the appropriate EMC classification for the intended environment.

Pluggable Equipment

For pluggable equipment, the socket outlet shall be installed near the equipment and shall be easily accessible.

Servicing

There are no user-serviceable parts inside these products. Any servicing, adjustment, maintenance, or repair must be performed only by service-trained personnel.

Note for Service Personnel

Caution: *There is a danger of a new battery exploding if it is incorrectly installed. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.*

Informations concernant la sécurité

Symbole de référence à la documentation. Si le produit est marqué de ce symbole, reportez-vous à la documentation du produit afin d'obtenir des informations plus détaillées.

WARNING Dans la documentation, un WARNING indique un danger susceptible d'entraîner des dommages corporels ou la mort.

CAUTION Un texte de mise en garde intitulé CAUTION indique un danger susceptible de causer des dommages à l'équipement.

Ne continuez pas au-delà d'une rubrique WARNING ou CAUTION avant d'avoir bien compris les conditions présentant un danger et pris les mesures appropriées.

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soient convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Attention: *Ce produit contient une pile au Lithium remplacable. Risque d'explosion si la pile est remplacee par un modele incorrect. Disposez des piles usagees selon les instructions.*

Hinweise zur Sicherheit

Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

WARNING Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

CAUTION Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

Fahren Sie nach dem Hinweis WARNING oder CAUTION erst fort, nachdem Sie den Gefahrenzustand verstanden und die entsprechenden Maßnahmen ergriffen haben.

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, daß der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfaßt, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, daß die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedienungspersonal durchgeführt werden.

Vorsicht: *Dieses Produkt enhalt eine wechselbare Lithium Batterie. Es besteht Explosionsgefahr wenn die Batterie durch einen falschen Typ ersetzt wird. Entsorgen Sie gebrauchte Batterien nach den Anweisungen.*

Considerazioni sulla sicurezza

Simbolo di riferimento alla documentazione. Se il prodotto è contrassegnato da questo simbolo, fare riferimento alla documentazione sul prodotto per ulteriori informazioni su di esso.

WARNING La dicitura WARNINGdenota un pericolo che può causare lesioni o morte.

CAUTION La dicituraCAUTION denota un pericolo che può danneggiare le attrezzature.

Non procedere oltre un avviso di WARNING o di CAUTIONprima di aver compreso le condizioni di rischio e aver provveduto alle misure del caso.

Questo prodotto è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegaento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Attenzione: *questo prodotto contiene batterie ricaricabili al Litio. Se vengono utilizzate delle batterie non adatte vi e' rischio di esplosione. Eliminare le batterie usate seguendo le istruzioni fornite a riguardo.*

Consideraciones sobre seguridad

Símbolo de referencia a la documentación. Si el producto va marcado con este símbolo, consultar la documentación del producto a fin de obtener mayor información sobre el producto.

WARNING Una WARNING en la documentación señala un riesgo que podría resultar en lesiones o la muerte.

CAUTION Una CAUTION en la documentación señala un riesgo que podría resultar en averías al equipo.

No proseguir después de un símbolo de WARNING o CAUTION hasta no haber entendido las condiciones peligrosas y haber tomado las medidas apropiadas.

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentación eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación o el juego de cable de alimentación suministrado. Si existe la probabilidad de que la protección a tierra haya sufrido desperfectos, desenchufar el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Curdado: *Este producto contiene pilas remplasables de Lithium. Riesgo de exposion si la pila es remplasada con el tipo incorrecto. Deseche la pilas usadas de accuerdo a las instrucciones.*

Safety Information (Japan)

安全性の考慮

安全記号

マニュアル参照記号。製品にこの記号がついている場合はマニュアルを参照し、注意事項等をご確認ください。

WARNING　マニュアル中の「WARNING」は人身事故の原因となる危険を示します。

CAUTION　マニュアル中の「CAUTION」は装置破損の原因となる危険を示します。

「WARNING」や「CAUTION」の項は飛ばさないで必ずお読みください。危険性に関する記載事項をよく読み、正しい手順に従った上で次の事項に進んでください。

これは安全性クラスIの製品で保護用接地端子を備えています。主電源から製品の入力配線端子、電源コード、または添付の電源コード・セットまでの間、切れ目のない安全接地が存在することが必要です。もしこの保護回路が損なわれたことが推測されるときは、接地が修復されるまで電源コードを外しておいてください。

LAN ケーブルの接地に関して:

- もし貴社のLANが複数の配電システムにより電力を受けている領域をカバーしている場合には、それらのシステムの安全接地が確実に相互に結合されていることを確認してください。
- LAN ケーブルは時として危険な過度電圧（例えば雷や、配電設備の電力網での障害）にさらされることがあります。露出した金属部分の取扱いには十分な注意をはらってください。

本製品の内部にはユーザーが修理できる部品はありません。サービス、調整、保守および修理はサービス訓練を受けた専門家におまかせください。

本製品には電源スイッチがありません。電源コードを接続したとき電源入となります。

CAUTION: この製品は交換可能なリチウム電池を使用しています。間違ったタイプに交換すると爆発の危険があります。使用済みの電池は説明書に従って処分して下さい。

Safety Information (China)

HP网络产品使用安全手册

使用须知

欢迎使用惠普网络产品，为了您及仪器的安全，请您务必注意如下事项：

1. 仪器要和地线相接，要使用有正确接地插头的电源线，使用中国国家规定 的 220V 电源。
2. 避免高温和尘土多的地方，否则易引起仪器内部部件的损坏。
3. 避免接近高温，避免接近直接热源，如直射太阳光、暖气等其它发热体。
4. 不要有异物或液体落入机内，以免部件短路。
5. 不要将磁体放置于仪器附近。

警告

为防止火灾或触电事故，请不要将该机放置于淋雨或潮湿处。

如果您按照以上步骤操作时遇到了困难，或想了解其它产品性能，请在以下网页上寻找相关信息：http://www.hp.com.cn

或联系我们

中国惠普有限公司
地址：北京建国路112号中国惠普大厦
电话： 010-65643888

注意: 此产品包括一可更换锂电池. 用错误型号电池更换会有爆炸危险. 务必按照说明处置用完的电池.

EMC Regulatory Statements

U.S.A.

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. Operation of this equipment in a residential area may cause interference in which case the user will be required to correct the interference at his own expense.

Canada

This product complies with Class A Canadian EMC requirements.

Australia/New Zealand

This product complies with Australia/New Zealand EMC Class A requirements.

Japan

VCCI Class A

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korea

사용자 안내문 : A 급기기

이기기는 업무용으로 전자파 적합등록을 받은 기기이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

BSMI

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Regulatory Model Identification Number

For regulatory identification purposes, the HP ProCurve Secure Access 700wl Series system components (Access Controller 720wl, Access Control Server 740wl, Integrated Access Manager 760wl) are assigned a Regulatory Model Number. The Regulatory Model Number for these components is RSVLC-0206.

This regulatory number should not be confused with the marketing name or product numbers (J8153A, J8154A, J8155A)

European Community

DECLARATION OF CONFORMITY
according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd.
Roseville, CA 95747-5502
U.S.A.

declares, that the product

Product Name: HP ProCurve Access Controller 720wl
HP ProCurve Access Control Server 740wl
HP ProCurve Integrated Access Manager 760wl

Model Number(s): J8135A, J8154A, J8155A

Regulatory Model: RSVLC-0206

Product Options: All

conforms to the following Product Specifications:

Safety: IEC 60950:1991 + A1, A2, A3, A4 / EN 60950:1992 + A1, A2, A3, A4, A11
IEC 60825-1:1993 / EN 60825-1:1994 + A11, Class 1 (Laser/LED)

EMC: CISPR 22:1997 / EN 55022:1998 Class A[1]
CISPR 24:1997 / EN 55024:1998
IEC 61000-3-2:1995 / EN 61000-3-2:1995 +A1, A2
IEC 61000-3-3:1994 / EN 61000-3-3:1995 +A1

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC, the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The Product was tested in a typical configuration with system peripherals from several manufacturers.

Roseville, June 12, 2003

Mike Avery, Regulatory Engineering Mgr.

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen (FAX: + 49-7031-14-3143)

INDEX

D

E

F

G

H

I

June 2004

Manual Part Number
5990-8806