HP ProCurve
Wireless Access Point 10ag

Installation and Configuration Guide

Publication Number

5991-8615
October 2007

Applicable Products

ProCurve Wireless Access Point 10ag NA	(J9140A)
ProCurve Wireless Access Point 10ag WW	(J9141A)

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.

Open Source Software Acknowledgement

This software incorporates open source components that are governed by the GNU General Public License (GPL). In accordance with this license, ProCurve Networking will make available a complete, machine readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:

Hewlett-Packard Company, L.P.
ProCurve Access Point 10ag
GNU GPL Source Code
Attn: ProCurve Networking Support
MS: 5551
Roseville, CA 95747 USA

Safety

Before installing and operating these products, please read the "Installation Precautions" in Chapter 2, "Installing the Access Point", and "Safety Information" in Appendix C, "Safety and EMC Regulatory Statements".

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5552
Roseville, California 95747-5552
http://www.hp.com/go/hpprocurve

Contents

1 Introducing the ProCurve Wireless Access Point 10ag

2 Installing the Access Point

3 Getting Started With Access Point Configuration

4 Setting Up the Access Point

5 Managing the Access Point

6 Troubleshooting

A Specifications

B Access Point Port and Network Cables

C Safety and EMC Regulatory Statements

C Open Source Licenses

D Recycle Statements

1

Introducing the ProCurve Wireless Access Point 10ag

The ProCurve Wireless Access Point 10ag is a dual-radio 802.11b/g and 802.11a access point that offers maximum flexibility in deployment and optimum throughput for high-density usage areas. Designed for small office/ home office (SOHO) environments, it provides high-speed, reliable wireless networking and comprehensive security and management features.

ProCurve Wireless Access Point 10ag NA (J9140A)
ProCurve Wireless Access Point 10ag WW (J9141A)

The Access Point 10ag has one 10/100Base-TX RJ-45 port. This port also supports Power over Ethernet (PoE) based on the IEEE 802.3af standard. The access point supports wireless connectivity at speeds up to 54 Mbps based on the IEEE 802.11g and IEEE 802.11a standards. This access point is designed to be used primarily for connecting wireless stations to a wired primary network.

This chapter describes the Access Point 10ag, including:

- Package Contents
- Front of the Access Point
- Back of the Access Point
- Access Point Features

Throughout this manual, the ProCurve Access Point 10ag will be referred to as the ‘access point’.

Package Contents

Before installing and using the access point, verify that the package you received is complete. A complete Access Point 10ag package includes the following items:

- *ProCurve Product Documentation CD-ROM*
  (contains PDF file copies of the documentation for the Access Point 10ag, including this *Installation and Configuration Guide*)
- Read Me First
- Customer Support/Warranty booklet
- Ethernet cable
- AC power adapter
- Four rubber feet

If any of the above items are damaged or missing, please contact the store from which you purchased the access point.

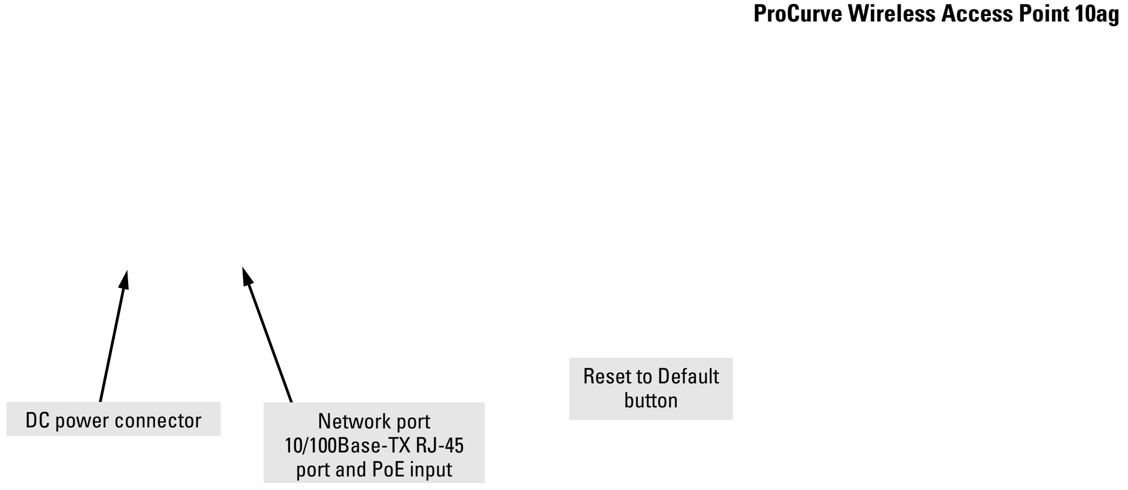
Front of the Access Point

LEDs on the Front Panel

Table 1-1. Access Point LEDs

LED Label	State	Meaning
Power	Green	The access point is receiving power.
	Off	The access point is NOT receiving power. If the power adapter is connected to a power source, verify that the power jack is connected properly to the power connector on the back panel of the access point.
Diag	Blinking amber	Reset to factory default is in progress. Blinking stops when the access point has completed resetting to factory defaults and is about to reboot. For more information on resetting to factory default using the Reset to Default button, refer to "Restoring Factory Default Configuration" on page 6-7.
	Off	Normal state
LAN	Off	The RJ-45 port has no network cable connected, or is not receiving a link signal.
	Blinking or solid green	The RJ-45 port has a link indication from a 10 Mbps or 100 Mbps device and is transmitting or receiving traffic. The LED blinking rate is proportional to the traffic rate. If there is no traffic, the blinking rate will be once every five seconds. As the traffic rate increases, the blinking rate also increases until the LED is solid on, which indicates there no available bandwidth on the port.
Link/Act (802.11a) Link/Act (802.11b/g)	Off	The wireless interface is disabled. For instructions on enabling the wireless interface, refer to "Configuring Advanced Wireless Settings" on page 4-25.
	Blinking or solid green	The wireless interface is enabled and transmitting or receiving traffic. The LED blinking rate is proportional to the traffic rate. If there is no traffic, the blinking rate will be once every second. As the traffic rate increases, the blinking rate also increases until the LED is solid green, which indicates there no available bandwidth on the interface.

Back of the Access Point


ProCurve Wireless Access Point 10ag
Reset to Default button
DC power connector
Network port 10/100Base-TX RJ-45 port and PoE input

LAN Port

The access point includes one 10/100Base-TX port. This port uses the "HP Auto MDIX" feature, which means that you can use either a straight-through or a crossover twisted-pair cable to connect the access point to a switch, a hub or a workstation.

Power Connector

The access point does not have a power switch; it is powered on when connected to the AC power adapter, and the power adapter is connected to an active AC power source.

The access point's power adapter automatically adjusts to any voltage between 100-240 volts and either 50 or 60 Hz. There are no voltage range settings required.

Caution

Use only the AC power adapter supplied with the access point. Use of other adapters, including adapters that came with other ProCurve Networking products, may result in damage to the equipment.

The access point may also receive Power over Ethernet (PoE) from a switch or another network device that supplies power over the network cable based on the IEEE 802.3af standard.

Note that if the access point is connected to a PoE source device (through the LAN port) and a local power source (through the AC power adapter) at the same time, PoE will be disabled automatically.

Reset to Default Button

Use the Reset to Default button to reboot the access point or to restore the access point to factory default settings. To reach the button, you will need a pointed object, such as the tip of a ballpoint pen or a straightened paper clip.

- **Reboot the access point:** Rebooting the access point can help clear any temporary error conditions. To reboot the access point, press the Reset to Default button for one to three seconds. All the LEDs will go off (except the Power LED), then after another second, the LEDs will turn on and blink. Note that when the access point is rebooted, any associated wireless client will be disconnected temporarily. Connection will be restored automatically after the access point completes rebooting.

Caution!

Do NOT press the Reset to Default button for more than four (4) seconds. Doing so will restore all access point settings to factory default.

- **Restore to factory settings:** Restoring the access point to factory settings will clear all configuration changes you have made through the Web interface, including the IP address, access control list, etc. Use the this function if you want to completely reconfigure the access point. For instructions on how to restore the access point to factory default settings, Restoring Factory Default Configuration in Chapter 6, Troubleshooting.

Antennas

The access point includes internal diversity antennas for wireless communications. A diversity antenna system uses two identical antennas to receive and transmit signals, helping to avoid multipath fading effects. When receiving, the access point checks both antennas and selects the one with the strongest signal. When transmitting, it will continue to use the antenna previously selected for receiving. The access point never transmits from both antennas at the same time.

Access Point Features

The wireless features of the Access Point 10ag include:

- dual-radio design with IEEE 802.11g/b and IEEE 802.11a radios
- supports up to 54 Mbps data rate on the wireless interface
- supports10/100Mbps data rate on the Ethernet interface with auto MDI/ MDIX
- worldwide roaming for 802.11d
- supports up to eight (8) Service Set IDentifier (SSID) interfaces
- independent security settings per SSID interface
- supports up to 128 wireless stations per radio interface
- advanced security through 64/128/152-bit WEP encryption, Wi-Fi Protected Access (WPA and WPA2), IEEE 802.1X, remote authentication via a RADIUS server, and MAC address filtering features to protect your sensitive data and authenticate only authorized users to your network
- access control list
- secured authentication of wireless clients through the client's Web browser
- dual power source options, including AC current and PoE (IEEE802.3af)
- reset to factory default parameters.
- enable and disable reset button

The other basic features of the Access Point 10ag include:

- one 10/100Base-TX RJ-45 port
- supports Power over Ethernet based on the IEEE 802.3af standard
- full-duplex operation for the 10/100 RJ-45 port
- easy management through a built-in graphical interface that can be accessed from common Web browsers (includes support for secure HTTP connections)
- RADIUS Accounting for logging user activity on the network
- download of new access point software for product enhancements or software updates
- backing up and restoring of configuration file

2

Installing the Access Point

The access point is easy to install. This chapter provides information on the requirements for installing the access point and guides you through the steps required for the proper installation of the device.

Topics covered include:

Before You Begin

Before starting with the installation, make sure that you have the required items for the installation ready. In addition, verify that the wireless stations on the network have the required components for wireless communication with the access point.

Installation Requirements

To install the access point, you need the following:

- Access point
- Power adapter (included in the access point package)
- Ethernet cable (included in the access point package)

If the default IP address **192.168.1.11** is not compatible with your network settings, you will need to change it before installing the access point. To change the IP address, you will need to connect a computer with TCP/IP and a 10Mbps or 100Mbps network interface card directly to the access point. This computer must also have a Web browser that supports JavaScript, such as Netscape 4.7 or later, Internet Explorer 5.0 or later, or Mozilla 1.2.1 or later.

The access point may also receive Power over Ethernet (PoE) from a switch or other network device that supplies power over the network cable based on the IEEE 802.3af standard. If you want to use PoE to supply power to the access point, you will also need an IEEE 802.3af-compliant power sourcing equipment (PSE).

Wireless Station Requirements

For wireless stations on the network to be able to communicate with the access point, they must have at least the following:

- An operating system that supports TCP/IP networking protocols (for example, Windows 95/98/NT/Me/2000/XP, UNIX, Mac OS 8.5 or later).
- An 802.11g, 802.11b, or 802.11a wireless network interface card

Safety Information

Before you continue, read the Appendix C, “Safety and EMC Regulatory Statements” on page C-1.

Installation Precautions

Follow these precautions when installing the access point:

Cautions

- Use only the AC power adapter supplied with the access point. Use of other adapters, including adapters that came with other ProCurve Networking products, may result in damage to the equipment.
- You can alternatively power the access point through a network connection to a switch or other network connection device that provides Power over Ethernet. However, note that if the access point is connected to a power source using its AC power adapter, Power over Ethernet is disabled.
- Make sure that the power source circuits are properly grounded, then use the power adapter supplied with the access point to connect it to the power source.
- When using the access point's AC power adapter, note that the AC outlet should be near the access point and should be easily accessible in case the access point must be powered off.
- Ensure that the access point does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add together the ampere ratings of all devices installed on the same circuit as the access point and compare the total with the rating limit for the circuit. The maximum ampere ratings are usually printed on devices near the AC power connectors.

- When using either the AC power adapter or PoE power, do not install the access point in an environment where the operating ambient temperature might exceed 40°C (104°F).
- Make sure the air flow around the sides of the access point is not restricted.

Summary of Installation Tasks

Follow these easy steps to install your access point. The rest of this chapter provides details on these steps.

1. **Preconfigure the access point** *(*page 2-4*)*. The access point ships with a default IP address of **192.168.0.11** and a subnet mask of **255.255.255.0**. If this IP address is already assigned to another device on the network or if the IP address settings are not compatible with your network, you will need to configure its IP address before installation.

2. **Prepare the installation site (**page 2-8**).** Make sure that the physical environment into which you will be installing the access point is properly prepared, including having the correct network cabling ready to connect to the access point and having an appropriate location for the access point. *Refer to page 2-4 for some installation precautions.*

3. **Verify that the access point completes its system initialization (**page 2-10**).** This is a simple process of plugging the access point into a power source, or connecting it to a switch that provides Power over Ethernet (PoE), and observing that the LEDs on the access point's front panel indicate correct access point operation.

4. **Position the access point (**page 2-11**).** The access point can be installed on a flat surface, such as a desktop, or mounted on a wall (mounting screws and bracket are not included in the access point package).

5. **Connect the power to the access point (**page 2-12**).** Once the access point is mounted, plug it into a nearby main power source using the supplied AC adapter, or connect it to a switch that provides Power over Ethernet.

6. **Connect to the network (**page 2-13**).** Using the appropriate network cable, connect the access point to a network connection point, such as a switch. The network connection can also be used to provide power to the access point through its PoE feature.

At this point, your access point is fully installed. See the rest of this chapter if you need more detailed information on any of these installation steps.

Installation Procedures

Step 1. Preconfigure the Access Point

In its factory default configuration, the access point is assigned a static IP address of **192.168.1.11** and a subnet mask of **255.255.255.0** (the built-in DHCP client is disabled).

- If your network uses the same IP address class or range, and the IP address **192.168.1.11** is not assigned to any other network device, you do not need to change the IP address settings of your access point. Continue to the next step, "Step 2. Prepare the Installation Site" on page 2-8
- If your network uses a different IP address class or range, you will need to change the IP address settings of the access point so that it can work on your network. Refer to the instructions below.

a. Prepare the Management Computer

You will need to prepare a management computer that you want to use to preconfigure the access point. The management computer must have the following minimum specifications:

- Network interface card with TCP/IP installed
- Microsoft Internet Explorer 6 (or later) or Mozilla Firefox 1.0 (or later)

Note

The following instructions are for preparing a management computer running Microsoft Windows XP. If your computer is running a different version of Windows, the procedures may vary slightly.

To prepare the management computer:

1. Choose a computer on your local network that you want to use to access and manage the access point.
2. On this computer, click **Start** > **Connect to** > **Show all connections**. The Network Connections window appears.
3. Right-click **Local Area Connection**, and then click **Properties**. The Local Area Connection Properties window appears.

4. Click **Internet Protocol (IP)**, and then click **Properties**.

Note

Remember to write down your computer's current IP address settings. You will need to change them back after you configure the IP address settings of the access point.

5. On the General tab of the Internet Protocol (IP) Properties window, click **Use the following IP address**.
6. In **IP address**, type an IP address that is on the same range as the default IP address (**192.168.1.11**) of the access point. For example, you can type **192.168.1.13**.
7. In **Subnet mask**, type **255.255.255.0**.
8. Click **OK**.

You are now ready to connect the management computer to the access point.

b. Connect the Management Computer to the Access Point

In this step, you will physically connect the management computer to the access point to prepare for preconfiguration.

1. Connect one end of the Ethernet cable that is supplied with the access point to the LAN port on the management computer.
2. Connect the other end of the Ethernet cable to the LAN port on the back panel of the access point.
3. Connect the supplied power adapter to the power connector on the back of the access point.
4. Connect the other end of the power adapter to a power source.

The LEDs on the front panel of the access point flash as the device boots up. When it has completed booting up, check the LEDs again:

- The Power LED should be green.
- One LAN LED - either Link/Act (100M) or Link/Act (10M) - should be green.
- Both Wireless LEDs should be blinking green (since both are enabled by default).

c. Connect to the Web Interface and Change the IP Address

1. Start your Web browser.
2. In the address or location bar, enter **http://192.168.1.11**. The logon dialog box appears.

3. In **User Name**, type **admin**.
4. In **Password**, type **password**. The Web interface appears, showing the Information page.
5. On the menu, click **Basic Settings**.
6. Configure the IP address settings.
   - (Recommended) If you want to assign a fixed IP address to the access point, select **Disable** in DHCP Client, and then enter the IP Address, IP Subnet Mask, and Default Gateway that you want to assign to it. These settings must be compatible with your network to ensure that the access point can communicate with other network devices.
   - If you have a DHCP server on the network and you want the access point to automatically obtain an IP address from the DHCP server, click Enable in DHCP Client. You do not have to configure other settings, but you will need to check the DHCP server periodically to determine the IP address that the access point is using.
7. (Applicable to Access Point 10ag WW only) In **Country/Region**, select the country where you are operating the access point. Available options include:
   - None (default)
   - Africa
   - China
   - Australia
   - Canada
   - Germany
   - Israel
   - Japan
   - Korea
   - Mexico
   - South America
   - USA

Note

- The **Country/Region** option is unavailable in Access Point 10ag NA. The country is fixed to USA.
- If you are using Access Point 10ag WW, you must select the correct country/region for the location in which you operate the access point, so that it uses the correct authorized radio channels for wireless network devices.

8. Click **Apply**.

You have completed configuring your access point's IP address settings so that it can work on your network. Remember to change your computer's IP address settings to its original settings.

Disconnect the access point from the management computer. You are now ready to find a suitable location for the access point and to connect the access point to the network.

Step 2. Prepare the Installation Site

Cabling Infrastructure

Ensure that the cabling infrastructure meets the necessary network specifications. Refer to Table 2-1 for cable types and lengths. For more information, refer to Appendix B, "Access Point Port and Network Cables" on page B-1.

Table 2-1. Summary of Cable Types to Use With the Access Point

Port Type	Cable Type	Length Limits
	Twisted-Pair Cables	
10/100Base-TX	• **10 Mbps operation:** Category 5, 100-ohm unshielded twisted-pair (UTP) • **100 Mbps operation:** Category 5, 100-ohm UTP cable.	100 meters **Note:** Since the 10Base-T operation is through the 10/100Base-TX port on the access point, if you ever want to upgrade the ports on other devices to 100Base-TX, it would be best to cable the 10/100Base-TX port on the access point initially with category 5 cable.

Installation Location

Before installing the access point, plan its location and orientation relative to other devices and equipment:

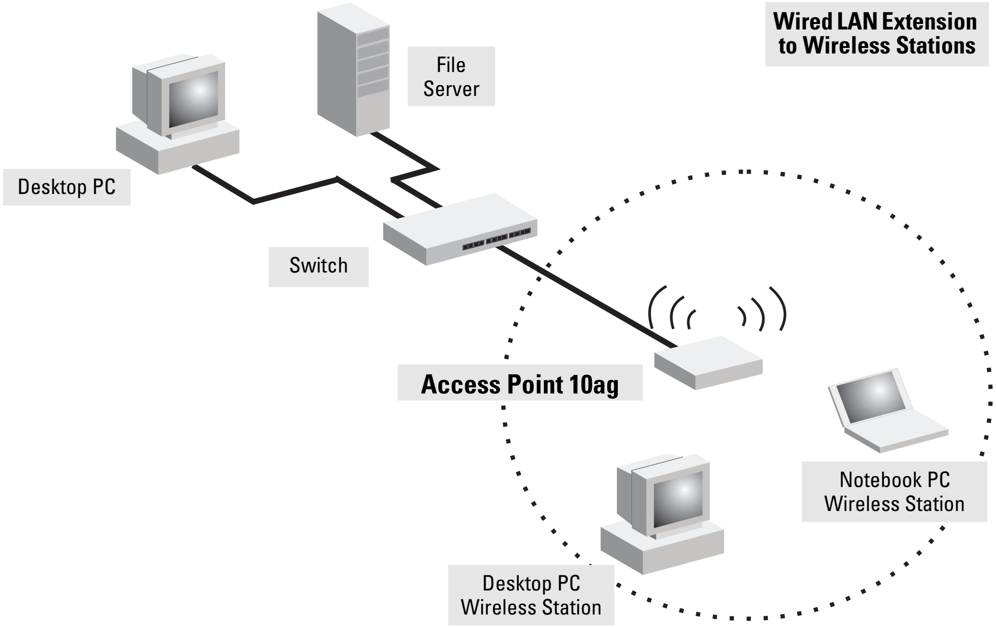
- Try to place the access point in the center of your wireless network. Normally, the higher you place the antennas, the better the performance. You may need to reposition the access point after testing the signal strength on several wireless stations to ensure that the access point's location provides optimal reception throughout the service area.
- Choose a location that allows easy viewing of the front panel LEDs and access to the port and connector on the back panel.
- At the back of the access point, leave at least 7.6 cm (3 inches) of space for the twisted-pair cabling and the power cord.
- On the sides of the access point, leave at least 7.6 cm (3 inches) for cooling.

Network Topology

The Access Point 10ag is designed to provide wireless stations access to a wired LAN. An integrated wired and wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users and an access point that is directly connected to the wired LAN. Each wireless PC in a BSS can communicate with any computer in its wireless group, or access other computers or network resources in the wired LAN through the access point.

The infrastructure configuration extends the accessibility of wireless PCs to the wired LAN and can be used for access to central network resources, or for connections between mobile workers, as shown in the following figure.

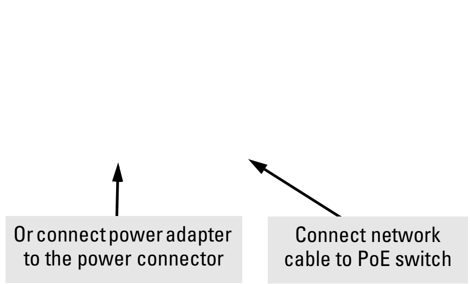
Figure 2-1. Infrastructure Wireless LAN


Wired LAN Extension to Wireless Stations
File Server
Desktop PC
Switch
Access Point 10ag
Notebook PC Wireless Station
Desktop PC Wireless Station

Step 3. Verify the Access Point Completes Initialization

Before deploying the access point to its network location, you should first verify that it is working properly by plugging it into a power source, or connecting it to a switch that provides Power over Ethernet, and verifying that it completes its system initialization.

1. Connect a network cable from a PoE source device (such as a switch) to the RJ-45 port on the back of the access point, or connect the supplied power adapter to the power connector on the back of the access point, and then into a properly grounded electrical outlet.



Or connect power adapter to the power connector

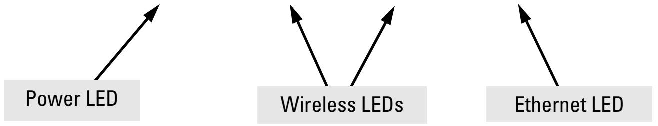
Connect network cable to PoE switch

Note

The Access Point 10ag does not have a power switch. It is powered on when the power adapter is connected to the access point and to a power source, or when a network cable is connected to the access point and to a network device that provides Power over Ethernet. For safety, when connecting to an electrical outlet, the power outlet should be located near the access point.

Use only the AC power adapter supplied with the access point. Use of other adapters, including adapters that came with other ProCurve Networking products, may result in damage to the equipment.

2. Check the LEDs on the access point as described below.



When the access point is powered on, it performs its system initialization. The system initialization takes between 30 seconds and one minute to complete.

LED Behavior

During the system initialization:

- The Power LED first turns on immediately, then one LAN LED (either 10M or 100M, depending on the speed of the connected device) turns on, and then the two Wireless LEDs turn on and off several times during the initialization phase.

When the system initialization completes successfully:

- The **Power** LED remains green.
- The **LAN** and **Wireless** LEDs on the front panel of the access point go into their normal operational mode:
  – If the RJ-45 network port and radio interfaces are connected to active network devices, the LEDs should be blinking at a rate proportional to the traffic rate. If there is no network activity, the LEDs should still be blinking at approximately 5 second intervals.
  – If the RJ-45 network port is not connected to an active network device and the radio interfaces are disabled, the LEDs should be off.

If the LED display is different than what is described above, the system initialization has not completed correctly. Refer to Chapter 6, "Trouble-shooting" for diagnostic help.

Step 4. Position the Access Point

Unplug the access point from its power source, and then place it in the network location that you have chosen. The access point can be installed on a flat surface (for example, on a desktop) or wall-mounted (mounting kit not included). When deciding where to position the access point, choose a location that:

- Allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.
- Is centrally located to the wireless computers that will connect to the access point. A suitable location might be on top of a high shelf or similar furniture to optimize wireless connections to computers in both horizontal and vertical directions, allowing wider coverage.

When positioning the access point, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- There are no thick walls or metal shielding between the access point and the wireless stations. In ideal conditions, the access point has a range of around 100 meters. If there are any obstructions between the wireless devices, the range is reduced and transmission speed is lower, .
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. HP recommends a minimum of 25 mm (1 in.) clearance.

Step 5. Connect the Access Point to a Power Source

1. Plug the included power adapter into the access point's power connector and into a nearby AC power source.

   Alternatively, connect the Ethernet port on the access point to a switch or other network device that provides Power over Ethernet.

Note

If you connect the access point to an AC power source and a PoE power source at the same time, PoE will be disabled.

2. Re-check the LEDs during the system initialization. See "LED Behavior" on page 2-11.

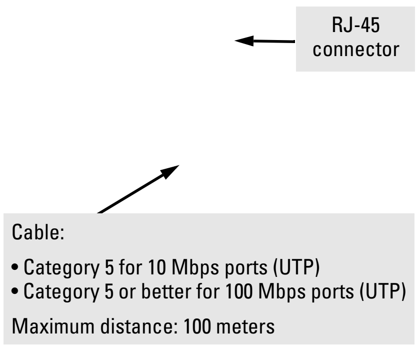
Step 6. Connect the Network Cable

Connect the network cable, described under "“Cabling Infrastructure” on page 2-8, from the network device or your patch panel to the LAN port on the access point.

Using the RJ-45 Connectors

To connect:
Push the RJ-45 plug into the LAN port until the tab on the plug clicks into place. When power is on for the access point and for the connected device, the 10/100Base-TX link LED should light to confirm a powered-on device (for example, a switch) is at the other end of the cable.

If the 10/100Base-TX link LED does *not* go on when the network cable is connected to the port, see “Diagnosing with the LEDs” in Chapter 5, “Troubleshooting”.



RJ-45 connector

Cable:

- Category 5 for 10 Mbps ports (UTP)
- Category 5 or better for 100 Mbps ports (UTP)

Maximum distance: 100 meters

To disconnect:
Press the small tab on the plug, and then pull the plug out of the port.

Congratulations! You have completed installing your access point. You are now ready to start configuring your access point settings.

Please continue to Chapter 3, “Getting Started With Access Point Configuration” on page 3-1 for an introduction of the Web interface and a summary of essential configuration tasks that HP recommends you perform.

Getting Started With Access Point Configuration

This chapter is a guide for logging on to the the Web interface and provides a summary of the essential configuration tasks you need to perform to get the access point up and running on your network.

Topics discussed include:

- Introducing the Management Web Interface
- Tasks for Your First Web Browser Interface Session
- Default Configuration Parameters

Introducing the Management Web Interface

The access point is managed through a graphical, Web browser-based interface that you can access from any PC or workstation on the same subnet as the access point. Open a compatible browser and type the access point's IP address as the URL. (See "Step 1. Preconfigure the Access Point" on page 2-4 for information on setting the IP address.)

Note

You can use the Web browser interface to access IP addressing only if the access point already has an IP address that is reachable through your network.

No additional software installation is required to make this interface available; it is included in the access point's onboard software.

The operating and Web systems support recommended to manage the access point through the browser interface are as follows:

- Microsoft Internet Explorer version 5.5 or later on Microsoft Windows Vista, Microsoft Windows XP, or Microsoft Windows 2000
- Netscape Mozilla 1.7.x on Redhat Linux version 2.4
- Mozilla/5.0 (Windows; U; Windows NT 5.1; rv:1.7.3) Gecko/20041001 Firefox/0.10.1

The Web browser that you will use for administration must have JavaScript enabled to support the interactive features of the Web interface. It must also support HTTP uploads to use the firmware upgrade feature.

Note

To ensure proper screen refresh when using Internet Explorer with Windows XP, be sure that the browser options are configured as follows: Under the menu "**Tools** > **Internet Options** > **Temporary Internet Files** > **Settings**," the setting for item "**Check for newer versions of stored pages**" should be set to"**Automatically**."

s

Logging On to the Web Interface

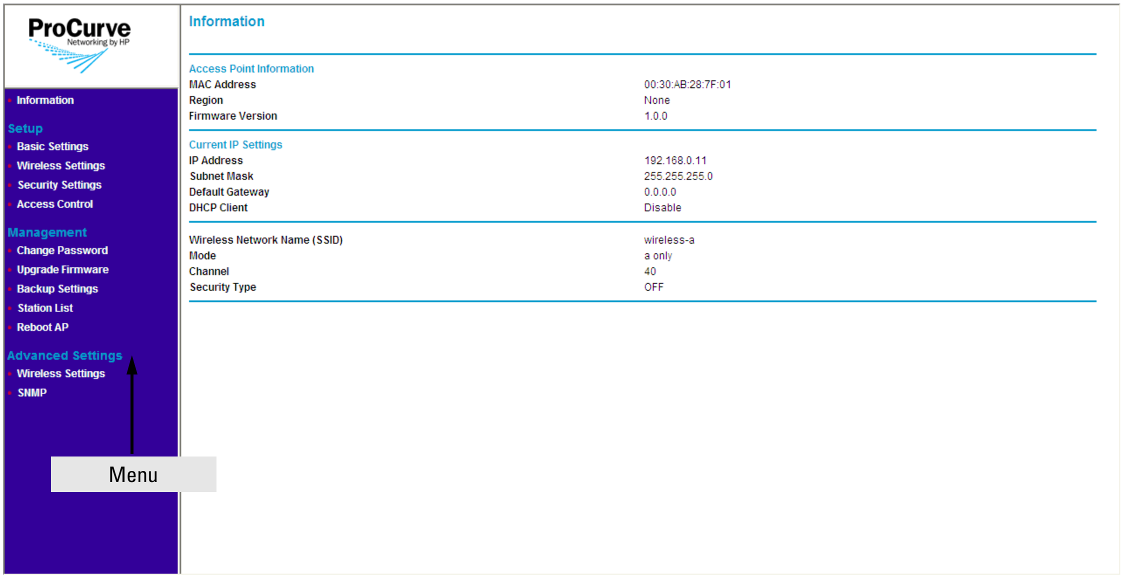
To log on to the Web interface:

1. Start your Web browser.
2. In the address or location bar, enter the IP address that you assigned to the access point when you preconfigured it in "Step 1. Preconfigure the Access Point" on page 2-4.

   A logon dialog box appears.
3. In **User name**, type **admin**.
4. In **Password**, type **password**.
5. Click **OK** to log on.

The ProCurve Access Point 10ag Web interface appears, showing the Information page.

Figure 3-1. Information Page (Web Interface Home Page)



Information

Access Point Information

MAC Address	00:30:AB:28:7F:01
Region	None
Firmware Version	1.0.0

Current IP Settings

IP Address	192.168.0.11
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disable

Wireless Network Name (SSID)	wireless-a
Mode	a only
Channel	40
Security Type	OFF

Note

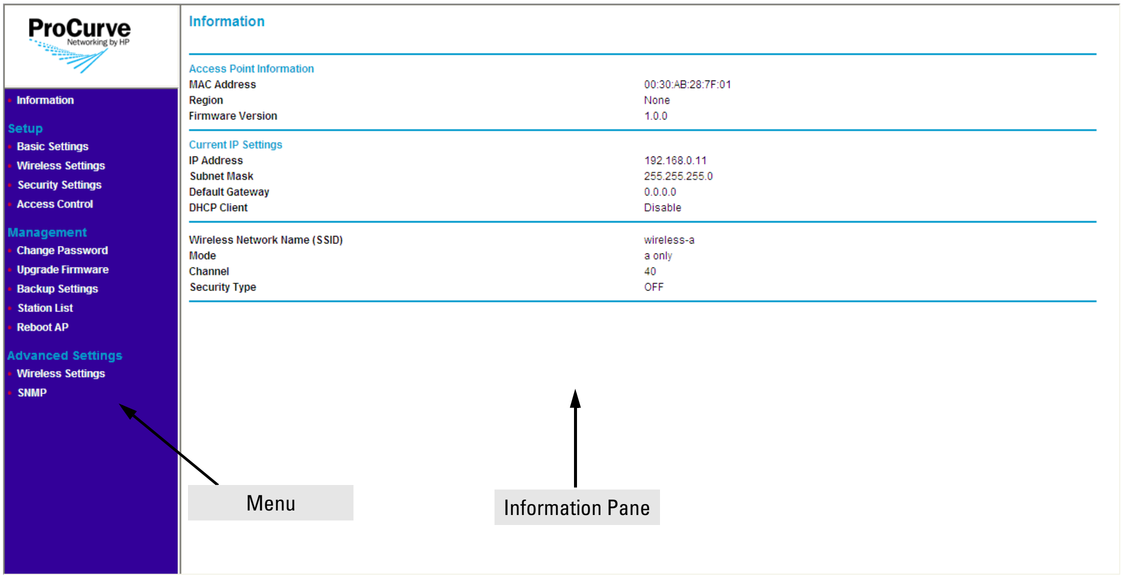
The Web interface does not have a Log Off button. To end your Web interface session safely, HP recommends closing the Web browser.

Navigating Around the Web Interface

The Web interface provides logical window groups for easy access to common setup, management, and advanced configuration features. This section details each of the logical window groups, submenus, screen elements and parameters. Cross-references are provided to any configuration procedures.

The Information sash is the first logical group available on the Web interface menu. Clicking the Information menu Once accessed, it defaults to the Information window, also considered the Access Point 10ag home page.

Figure 3-2. Web Interface Elements



Information

Access Point Information

MAC Address	00:30:AB:28:7F:01
Region	None
Firmware Version	1.0.0

Current IP Settings

IP Address	192.168.0.11
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disable

Wireless Network Name (SSID)	wireless-a
Mode	a only
Channel	40
Security Type	OFF

The Web interface has two primary sections:

- **The menu**: Located on the left-hand side of the page, the menu contains links to the primary configuration options on the Web interface. Menu items are grouped into four categories:
  - **Information** (default home page): Shows information about the access point, including the MAC address, firmware version, current IP address settings, and configured wireless networks.
  - **Setup**: Contains options for configuring the essential access point settings, such as basic IP address settings, basic wireless settings, security settings, and access control.
  - **Management**: Contains options for performing administrative tasks on the access point, including changing the password, uprading the firmware, backing up and restoring settings, viewing the list of associated wireless stations, and rebooting the access point.
  - **Advanced Settings**: Contains options for configuring advanced wireless radio settings and changing the SNMP community names used by the access point.
- **The information pane**: Shows related configuration options for each item on the menu. For example, if you click **IP Settings** on the menu, the information pane loads the parameters that you can set or edit, and then save for your desired configuration change to take effect.

Tasks for Your First Web Browser Interface Session

The first time you access the Web browser interface, there are a number of basic tasks that you should perform. Table 3-1 lists these essential tasks. For specific instructions on the how perform the procedure, refer to the page number listed in the right column.

In setting up your access point for network installation, this manual covers many of the tasks that should be considered for proper security and management.

Each of these tasks are detailed in their respective sections, however, this summary is provided as an aid for establishing your network.

Table 3-1. Basic Web Interface Tasks

To Learn How to Do This Task	Refer to
Change the default password	"Changing the Management Password" on page 5-3
Set the correct country code	"Configuring Basic Settings" on page 4-1
Control access to the wireless network	"Controlling Access to the Wireless Network" on page 4-22
Setting WLAN security to utilize WPA/WPA2	"Configuring the Security Settings" on page 4-7

Default Configuration Parameters

Table 3-2 lists some of the default settings with which the access point is configured, including the basic IP address and wireless configuration parameters. Information on how to update each parameter is provided later in this guide.

Table 3-2.

Parameter	Default	Description
Username	admin	The name of the manager.
Password	password	The password for the manager.
IP Address	192.168.1.11	IP address compatible with your network.
Subnet Mask	255.255.255.0	Subnet mask compatible with your network.
Default Gateway	*not set*	IP address of the next-hop gateway node for network traffic that needs to be able to reach off-subnet destinations.
Radio 1 Mode	802.11g	The operating mode for Radio 1.
Radio 2 Mode	802.11a	The operating mode for Radio 2.
SSIDs	wireless-g - SSID 1 wireless-a - SSID 2	The Service Set Identifier (SSID) for the access point interface, which is broadcast in the beacon frames.

Note: The IP address and subnet mask assigned to the access point must be compatible with the IP addressing used on your network. For more information on IP addressing, see "Configuring Basic Settings" on page 4-1.

Setting Up the Access Point

This chapter provides information on how configure the access point’s network, wireless, and security settings to ensure its proper operation on the network. It also describes how to configure advanced options, such as the wireless radio settings and the built-in SNMP agent.

Topics discussed in this chapter include:

- Configuring Basic Settings
- Configuring Basic Wireless Settings
- Configuring the Security Settings
- Controlling Access to the Wireless Network
- Configuring Advanced Wireless Settings

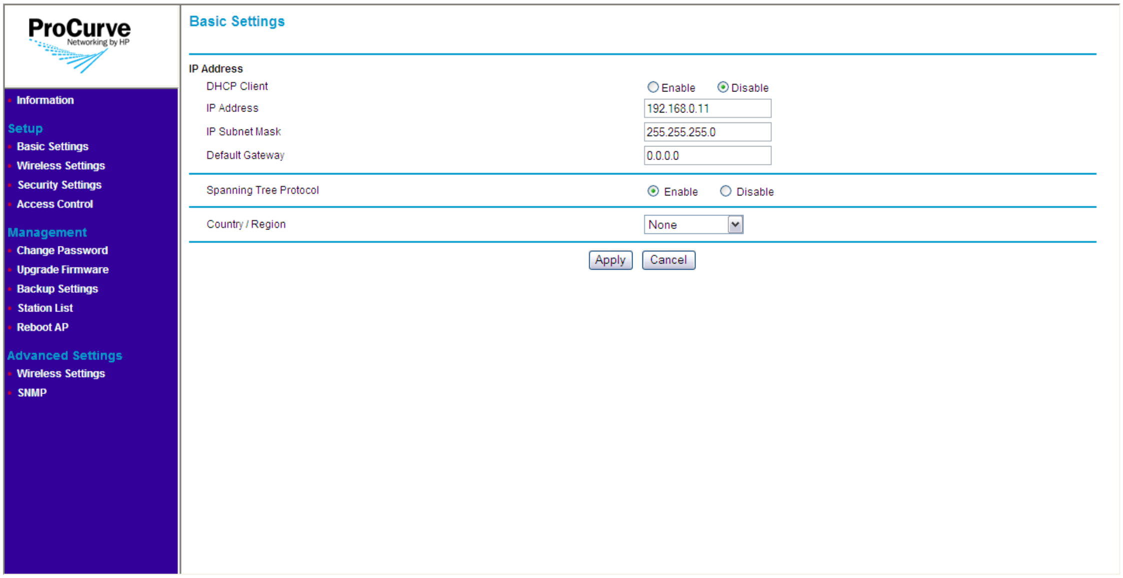
Configuring Basic Settings

Basic settings refer to the IP address settings and the country code assigned to the access point. Configuring the access point with an IP address The procedure for configuring your access point's IP settings depends on the network mode that you have selected.

Note

If the access point's IP address settings are already compatible with your network, you do not need to change them.

Figure 4-1. Basic Settings Page



Basic Settings

IP Address

DHCP Client	○ Enable ● Disable
IP Address	192.168.0.11
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Spanning Tree Protocol	● Enable ○ Disable
Country / Region	None

To configure the access point's basic settings:

1. On the menu, click **Basic Settings**.
2. Configure the IP address settings.
   - Assign an IP address (recommended) – If you want to assign a fixed IP address to the access point, select **Disable in DHCP Client**, and then enter the IP Address, IP Subnet Mask, and Default Gateway that you want to assign to it. These settings must be compatible with your network to ensure that the access point can communicate with other network devices.
   - Enable the built-in DHCP client – If you have a DHCP server on the network and you want the access point to automatically obtain an IP address from the DHCP server, click **Enable** in DHCP Client. You do not have to configure other settings, but you will need to check the DHCP server from time to time to determine the IP address that the access point is using. You need this IP address to connect to the Web interface.

Note

If you enable the built-in DHCP client and the access point fails to obtain an IP address from the DHCP server (for example, the DHCP server is unreachable), the access point will automatically use **192.168.1.11**, its default IP address.

3. If your network requires network devices to support the Spanning Tree Protocol (for example, if your network requires STP for redundancy), select the **Enable** button.
4. In **Country/Region**, select the country or region where you are installing the access point (if you have not done so earlier).

Notes

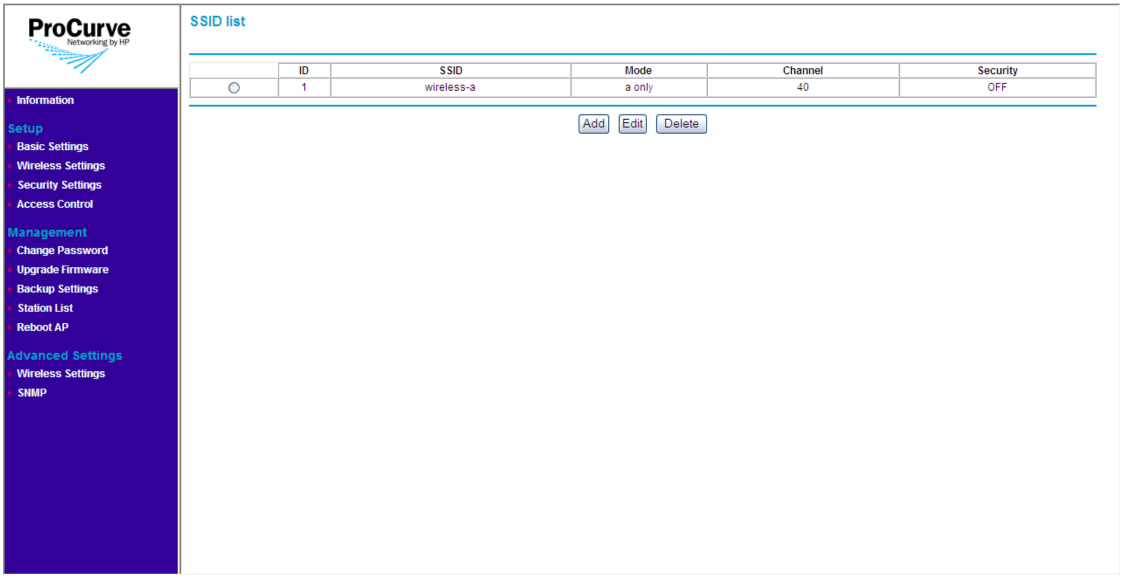
- The Country/Region option is unavailable in Access Point 10ag NA. The country is fixed to **USA**.
- If you are using Access Point 10ag WW, you must select the correct country/region for the location in which you operate the access point, so that it uses the correct authorized radio channels for wireless network devices.
- The radios are disabled if the Country/Region option is not set. Once this option is configured, the radios can be enabled.
- When resetting to factory defaults, the Access Point 10ag WW unit must have its Country/Region setting configured. The Access Point 10ag NA will be set to USA.

5. Click **Apply**.

Configuring Basic Wireless Settings

Basic wireless settings define the SSID, wireless channel, wireless mode, and data rate that each wireless interface uses. Each SSID or The access point comes with one predefined wireless profile (SSID **wireless-a**), which allows 802.11a wireless clients to associate with it. You can edit this existing wireless profile, or you can create a new one.

Figure 4-2. Basic Wireless Settings Page



SSID list

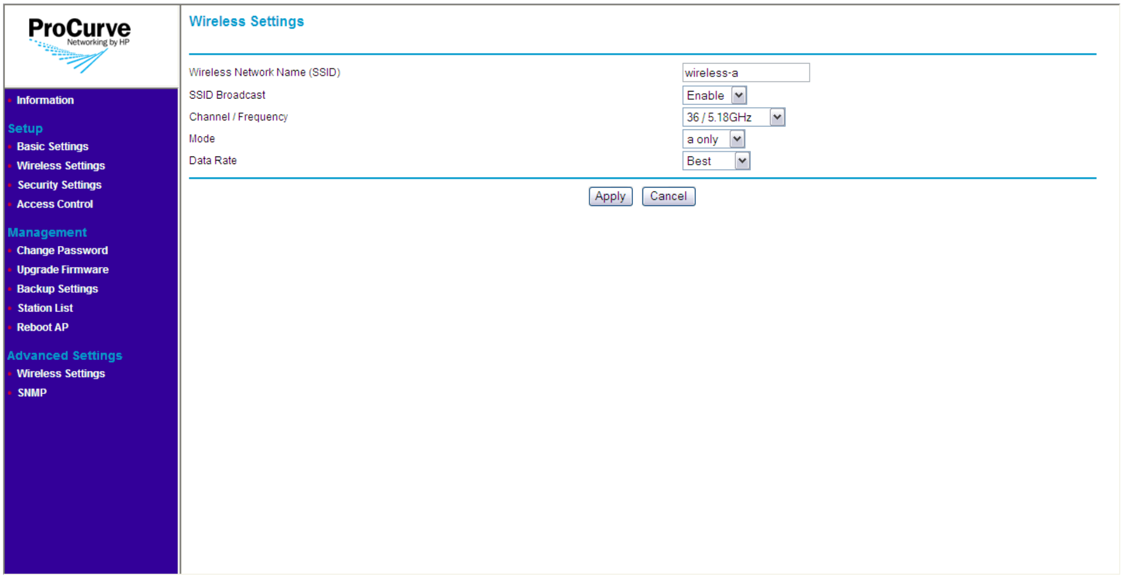
	ID	SSID	Mode	Channel	Security
○	1	wireless-a	a only	40	OFF

Creating a Wireless Profile

Note

The access point ships with one preconfigured wireless profile for 802.11a. You can create up to 8

Figure 4-3. Add Wireless Profile Page



Wireless Network Name (SSID): wireless-a
SSID Broadcast: Enable
Channel / Frequency: 36 / 5.18GHz
Mode: a only
Data Rate: Best

To create a new wireless profile:

1. On the menu, click **Wireless Settings** under **Setup**. The SSID List page appears.

2. Click **Add**. The Wireless Settings page appears.

3. In **Wireless Network Name (SSID)**, type a unique SSID (not used on your network) that you want to assign to the wireless profile.

4. In **SSID Broadcast**, select **Enable** if you want to allow all wireless stations within the range of the access point to see the SSID. Otherwise, click **Disable**.

5. In **Mode**, select the wireless mode that you want this wireless profile to use. Available options include:

   - **g and b**: Select to allow connections from 802.11g and 802.11b clients only.
   - **a**: Select to allow connections from 802.11a clients only.

6. In **Channel/Frequency**, select the wireless channel and frequency that you want this wireless profile to use. The range of channels and frequencies available depends on the wireless mode that you selected.

7. In **Data Rate**, select the maximum speed at which the access point can transmit traffic for this wireless profile. If you want the access point to automatically use the optimum data rate for the associated wireless stations, select **Best**.
8. Click **Apply**. A confirmation message appears.
9. Click **OK** to finish creating the wireless profile.

Editing a Wireless Profile

To edit an existing wireless profile:

1. On the menu, click **Wireless Settings** under **Setup**.
2. Click the option button for the wireless profile that you want to edit. For example, if you want to edit the **wireless-a** profile, click the option button next to it.
3. Click **Edit**.
4. Modify the following settings as required:
   - **Wireless Network Name (SSID)**
   - **SSID Broadcast**
   - **Channel/Frequency**
   - **Mode**
   - **Data Rate**
5. Click **Apply**.

Deleting a Wireless Profile

To delete a wireless profile:

1. On the menu, click **Wireless Settings** under **Setup**. The SSID List page appears.
2. Select the option button for the wireless profile that you want to delete.
3. Click **Delete**.

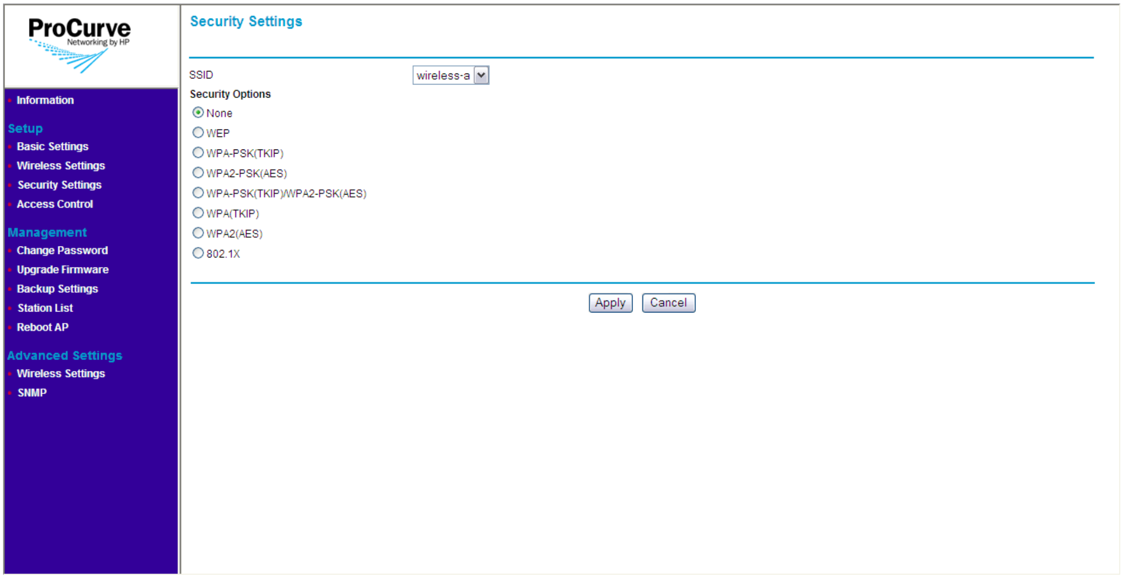
The message **Please wait...** appears. After a few seconds, the SSID List refreshes and the wireless profile you chose to delete disappears from the list of SSIDs.

Configuring the Security Settings

Unlike wired networks, anyone with a compatible wireless card can receive your wireless data transmissions well beyond your walls. Operating an unsecured wireless network creates an opportunity for outsiders to eavesdrop on your network traffic or to enter your network to access your computers and files. For this reason, use the security features of your wireless equipment.

Deploy the security features appropriate to your needs.

Figure 4-4. Security Settings Page



Security Settings

SSID: wireless-a

Security Options

● None
○ WEP
○ WPA-PSK(TKIP)
○ WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
○ WPA2(AES)
○ 802.1X

Wireless Security Overview

By default, the access point is configured as an “open system,” with no security. This means that the access point broadcasts a beacon frame advertising each configured wireless network (SSID). If a wireless client has a configured WLAN of "any," it can read the SSID from the beacon and use it to allow immediate connection to the access point. Client stations are permitted to connect with the access point without first verifying that users are authorized to access the network.

In addition, user data is transmitted over the air without being encrypted, and is subject to being intercepted by client stations anywhere within range that want to eavesdrop on the wireless network.

Wireless network security requires attention to three main areas:

- **Authentication**: Verifying that stations attempting to connect to the network are authorized users before granting access to the network.
- **Encryption**: Encrypting data that passes between the access point and stations (to protect against interception and eavesdropping).
- **Key Management:** Assigning unique data encryption keys to each wireless station session, and periodically changing the encryption keys to minimize risk of their potential discovery.

Authentication

The two ways of authenticating users on the Access Point 10ag are:

- MAC Authentication: Based on the user's wireless station MAC address.
- 802.1X Authentication: Based on the user credentials, such as; username/ password, digital certificates, etc.

MAC Authentication. MAC authentication of users can be done either using a remote authentication server like a RADIUS server or by creating a local database on the access point itself. MAC authentication is not as secure as 802.1X authentication, as it is easy to decipher and spoof for unauthorized network access.

802.1X Authentication. User 802.1X authentication can be implemented either using a remote authentication server, such as a RADIUS server or by using the local built-in RADIUS server on the access point itself. The user's credentials are exchanged with the servers (both remote and local built-in) using a mechanism called “Extensible Authentication Protocol (EAP)”. EAP is a public-key encryption system to ensure that only authorized network users can access the network. In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and sends back to the server to complete the authentication. Local built-in RADIUS server supports only one EAP type - PEAP-MSCHAPv2. For remote server authentication, the access point serves as an intermediate authenticator to transparently pass any EAP type to the remote server as specified in RFC3748.

The Access Point 10ag supports all EAP type tested by the WiFi Alliance; TLS, TTLS, PEAP0/MSCHAPv2, PEAP1/GTC and SIM. EAP types which do not provide key management (like MD5) are not suitable for wireless networks. 802.1X authentication can be used with WEP, TKIP and AES encryption ciphers. It is possible to use a combination of both MAC authentication and 802.1X authentication simultaneously on the same WLAN.

Encryption

The access point supports three types of encryption:

- Wired Equivalent Privacy (WEP): Key lengths of 64 bits and 128 bits are possible. WEP provides the least secure method of encryption (static WEP is not secure, as it can be easily compromised).
- Temporal Key Integrity Protocol (TKIP): Intermediate security between WEP and AES with key length of 256 bits. Provides a more-secure method of encryption than WEP (security is much better than WEP, but not as robust as AES).
- Advanced Encryption Standard (AES): AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks.

Key Management

Keys for encrypting the data can be managed either dynamically using 802.1X authentication or statically using pre-shared keys between the access point and station. Dynamic key management provides significantly better security when compared to using static keys.

Deciding Which Security Profile to Use

Table 4-1 shows a summary of available security profiles. Use this table as a reference when deciding on which security profile best suits your network.

Remember that certain security profiles may require additional software or hardware. 802.1X, for example, requires a RADIUS server to be configured on the network. Additionally, not all wireless network cards support WPA.

Choose a security profile that provides the highest level of security while maintaining compatibility with most, if not all, existing wireless devices on the network.

Table 4-1. Summary of Wireless Security

Security Profile	Client Support	Implementation Considerations
None (NOT RECOMMENDED)	Built-in support on all 802.11a, 802.11b, and 802.11g devices	No key management, data encryption, or user authentication is used
WEP	Built-in support on all 802.11a, 802.11b, and 802.11g devices	• Provides only weak security • Requires manual key management
WPA-PSK (TKIP)		•
WPA2-PSK (AES)		•
WPA-PSK (TKIP) / WPA2-PSK (AES)		•
WPA (TKIP)		•
WPA2 (AES)		•
802.1X		•

When you have decided on which security profile to implement on your network, refer to the next section, ”Configuring the Access Point with Your Preferred Security Profile”, for more details including the configuration procedures.

Configuring the Access Point with Your Preferred Security Profile

Wireless security options are available on the Security Settings page. By default, the Security Settings page shows **None** as the selected security profile. When you click other security options, the page refreshes, and then displays additional options for that security profile.

Note

The security profile for each SSID must be set separately. For example, if you set wireless-a to use **WPA2**, it will only be be applied to wireless-a. If you want other SSIDs to use WPA2 as well, you need to configure each one separately.

Caution!

When access point configuration parameters are changed, wireless stations may be temporarily disconnected until the new configuration parameter is enabled. This includes any changes to a WLAN or radio parameter.

Using No Security

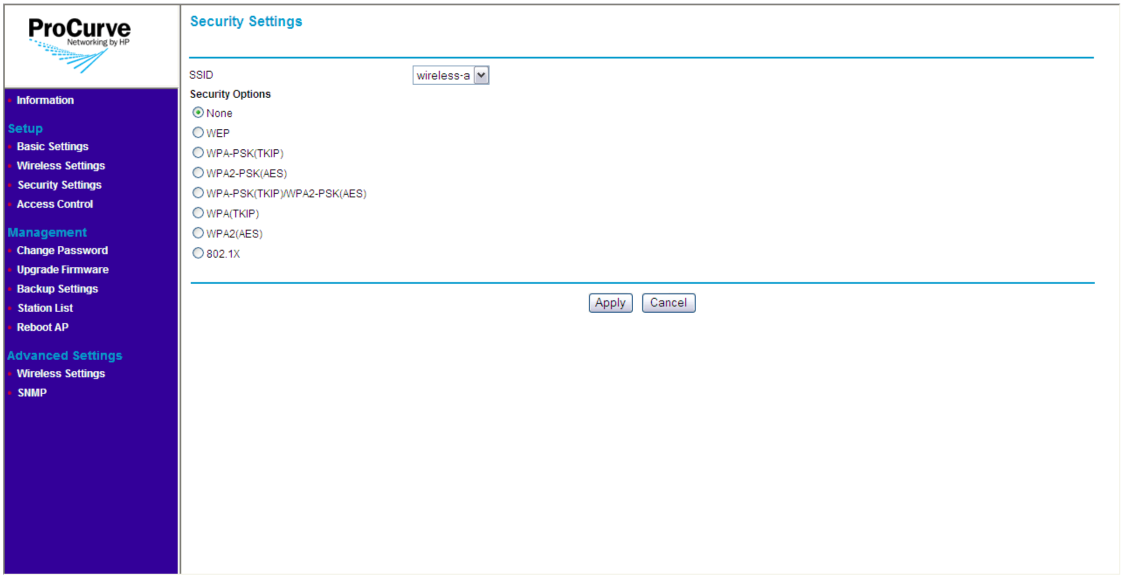
No security mode transmits data over the wireless connection without any form of encryption for data privacy. This mode may be appropriate for systems that provide simple internet and printer access, as on a guest network. It may also be appropriate where additional security is provided by the use of encrypted VPN tunnels between the wireless client device and a network VPN server. If this mode is used, it may be desirable to prevent advertising availability of the network to other stations by configuring the WLAN for closed-system operation.

Caution!

Use this mode on a sensitive internal network only for: initial setup, testing, or problem solving; or where VPN connections are mandated to provide endto-end security for the otherwise insecure wireless connection.

Setting Up the Access Point

Figure 4-5. No Security (Default) Page



Security Settings

SSID wireless-a

Security Options

● None
○ WEP
○ WPA-PSK(TKIP)
○ WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
○ WPA2(AES)
○ 802.1X

To use no security (not recommended):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under Security Options, click **None**.
4. Click **Apply** to save your changes.

Repeat this procedure for every SSID that you want to use no security.

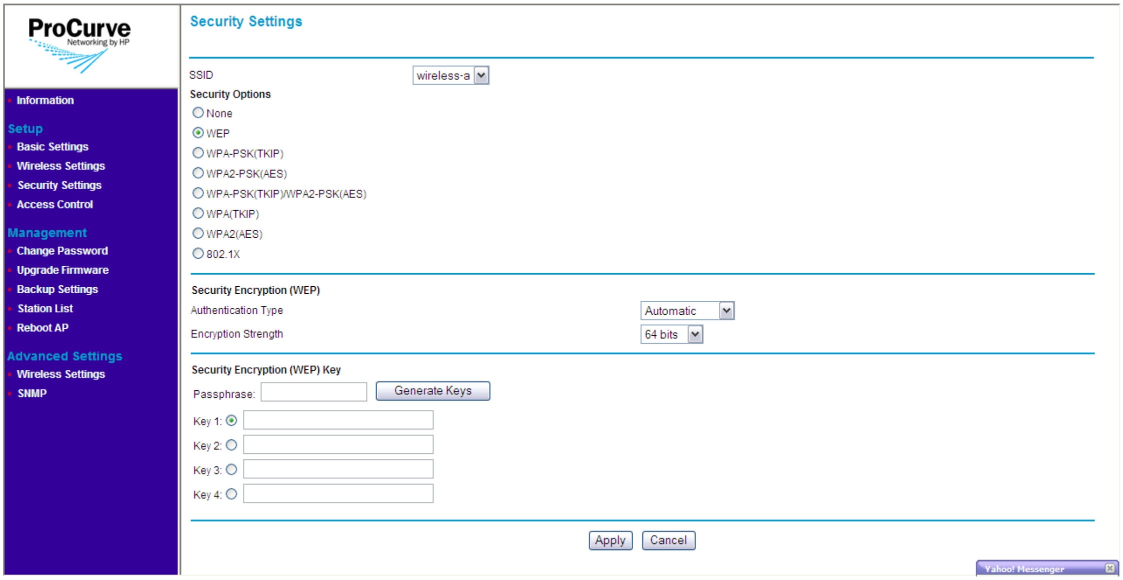
Configuring WEP

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the access point. WEP uses static shared keys (fixed-length alphanumeric strings) that are manually distributed to all clients that want to use the network.

Caution!

WEP has been found to be seriously flawed and is not be recommended for a high level of network security. For more robust wireless security, the access point provides Wi-Fi Protected Access (WPA or WPA2) for improved data encryption and user authentication.

Figure 4-6. WEP Options



Security Settings

SSID: wireless-a

Security Options
○ None
● WEP
○ WPA-PSK(TKIP)
○ WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
○ WPA2(AES)
○ 802.1X

Security Encryption (WEP)
Authentication Type: Automatic
Encryption Strength: 64 bits

Security Encryption (WEP) Key
Passphrase:
Key 1: ●
Key 2: ○
Key 3: ○
Key 4: ○

To use WEP:

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **WEP**.
4. Under **Security Encryption (WEP)**, configure the authentication type and encryption strength.
   - **Authentication**: Select **Open System** to allow association of wireless stations without requiring authentication. Select **Shared Key** to establish a rudimentary form of user authentication. Select **Automatic** if Shared Key authentication is to be supported, but not required. Default is Automatic.

Caution!

Shared Key mode is seriously flawed, in that it utilizes the static WEP encryption key (transmitted openly) for station authentication. This allows the WEP encryption key to be easily discovered by anyone who might eavesdrop on the wireless network. If static WEP is configured, it is recommended to select Open System authentication.

- **Encryption Strength**: Set the length of the encryption key that will be used. Select **64 bits** or **128 bits**. Note that the same size of encryption key must be supported on all wireless stations. Default is **64 bits**. 56tgb uh ik/

5. Under **Security Encryption (WEP) Key**, enter up to four strings of character keys. The number of characters required updates automatically based on how you set Authentication and Encryption Strength.
6. Click **Apply** to save your changes.

Configuring WPA-PSK (TKIP)

Wi-Fi Protected Access (WPA) is an early version of the 802.11i security standard. Temporal key integrity protocol (TKIP) is designed for WPA to enhance WEP.

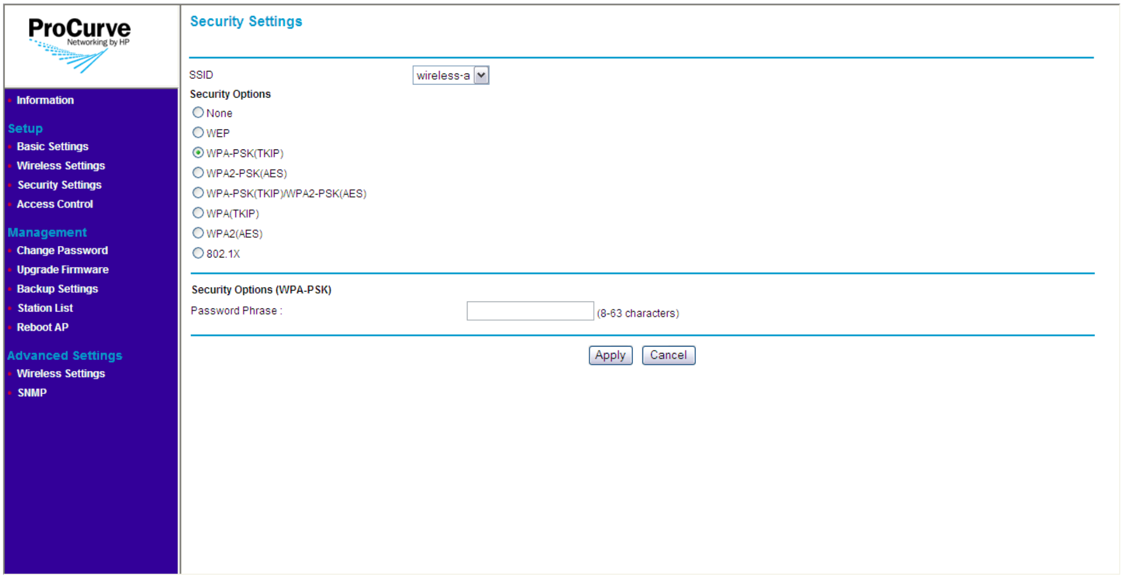
WPA-PSK (TKIP) employs a pre-shared key (PSK), which is used for an initial check of credentials and a 128-bit "temporal key", which combines the station’s MAC address and a 16-octet initialization vector to produce the encryption key. This ensures unique key encryption. TKIP uses RC4 to perform the encryption and changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network.

To use this security profile, your wireless stations must support WPA.

Note

If your wireless network has a mix of stations, some support WPA2 and others support the original WPA, HP recommends using WPA-PSK (TKIP)/WPA2-PSK (AES). Refer to “Configuring WPA-PSK (TKIP) / WPA2-PSK (AES)” on page 4-16 for more information.

Figure 4-7. WPA-PSK (TKIP) Options



Security Settings

SSID wireless-a

Security Options

○ None
○ WEP
● WPA-PSK(TKIP)
○ WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
○ WPA2(AES)
○ 802.1X

Security Options (WPA-PSK)

Password Phrase : (8-63 characters)

To use WPA-PSK (TKIP):

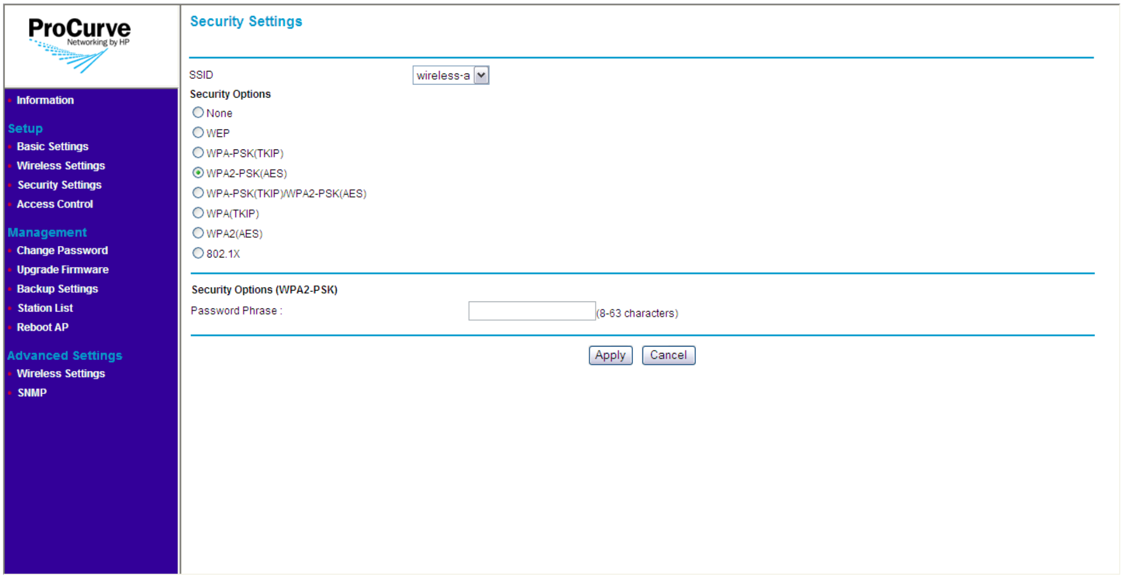
1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **WPA-PSK (TKIP)**.
4. In the **Password Phrase** box under Security Options (WPA-PSK), enter a string of at least 8 characters to a maximum of 63 characters. The string that you enter here will be used as the shared secret key for WPA-PSK.
5. Click **Apply** to save your changes.

Configuring WPA2-PSK (AES)

WPA2-PSK (AES) employs a pre-shared key (PSK), which is used for an initial check of credentials, and CCMP, an IEEE802.1X encryption method that uses the Advanced Encryption Algorithm (AES).

To use this security profile, your wireless stations must support WPA.

Figure 4-8. WPA2-PSK (AES) Options



Security Settings

SSID wireless-a

Security Options

○ None
○ WEP
○ WPA-PSK(TKIP)
● WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
○ WPA2(AES)
○ 802.1X

Security Options (WPA2-PSK)

Password Phrase : (8-63 characters)

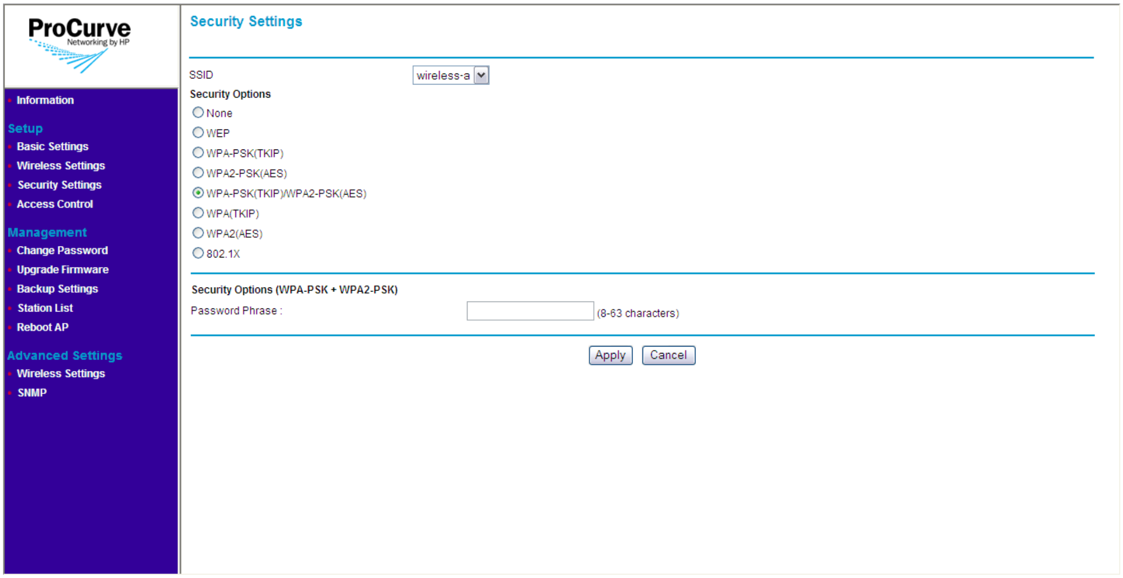
To use WPA2-PSK (AES):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **WPA2-PSK (AES)**.
4. In the **Password Phrase** box under Security Options (WPA-PSK), enter a string of at least 8 characters to a maximum of 63 characters. The string that you enter here will be used as the shared secret key for WPA-PSK.
5. Click **Apply** to save your changes.

Configuring WPA-PSK (TKIP) / WPA2-PSK (AES)

This security profile combines WPA-PSK (TKIP) and WPA2-PSK (AES). It uses a pre-shared key (PSK), which is used for an initial check of credentials, and a mixed cipher mode of TKIP and AES.

Figure 4-9. WPA-PSK (TKIP) / WPA2-PSK (AES) Options



Security Settings

SSID wireless-a

Security Options

○ None
○ WEP
○ WPA-PSK(TKIP)
○ WPA2-PSK(AES)
● WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
○ WPA2(AES)
○ 802.1X

Security Options (WPA-PSK + WPA2-PSK)

Password Phrase : (8-63 characters)

To use WPA-PSK (TKIP) / WPA2-PSK (AES):

1. On the menu, click **Security Settings**. The Security Settings page appears.

2. In **SSID**, select the SSID for which you want to set the security profile.

3. Under **Security Options**, click **WPA-PSK (TKIP) / WPA2-PSK (AES)**.

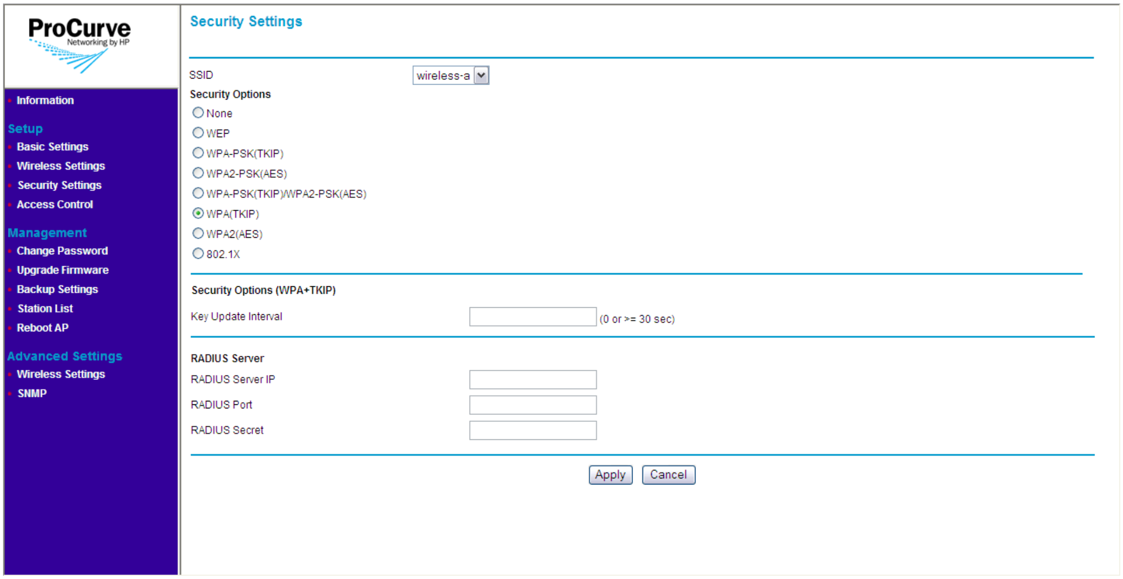
4. In the **Password Phrase** box under Security Options (WPA-PSK), enter a string of at least 8 characters to a maximum of 63 characters. The string that you enter here will be used as the shared secret key for WPA-PSK.

1. Click **Apply** to save your changes.

Configuring WPA (TKIP)

This security profile uses TKIP as the encryption cipher and 802.1X as the authentication mechanism. In this way, each station is going to utilize a unique master key to derive the encryption between the access point and station.

Figure 4-10. WPA (TKIP) Options



Security Settings

SSID: wireless-a

Security Options
○ None
○ WEP
○ WPA-PSK(TKIP)
○ WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
● WPA(TKIP)
○ WPA2(AES)
○ 802.1X

Security Options (WPA+TKIP)

Key Update Interval: (0 or >= 30 sec)

RADIUS Server
RADIUS Server IP:
RADIUS Port:
RADIUS Secret:

To use WPA (TKIP):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **WPA (TKIP)**.
4. In the **Key Update Interval** box, define the time interval (in seconds) for regenerating a group key.
5. Under RADIUS Server, configure the RADIUS server settings:
   - **RADIUS Server IP**: Type the IP address of the RADIUS server on the network.
   - **RADIUS Port**: Type the User Datagram Protocol (UDP) port number used by the RADIUS server for accounting messages. Setting the port number to zero disables RADIUS authentication.

- **RADIUS Secret**: Type a shared text string used to encrypt messages between the access point and the RADIUS server. Make sure that the same text string is specified on the RADIUS Accounting server. Do not use blank spaces in the string. (Maximum length: 20 characters)

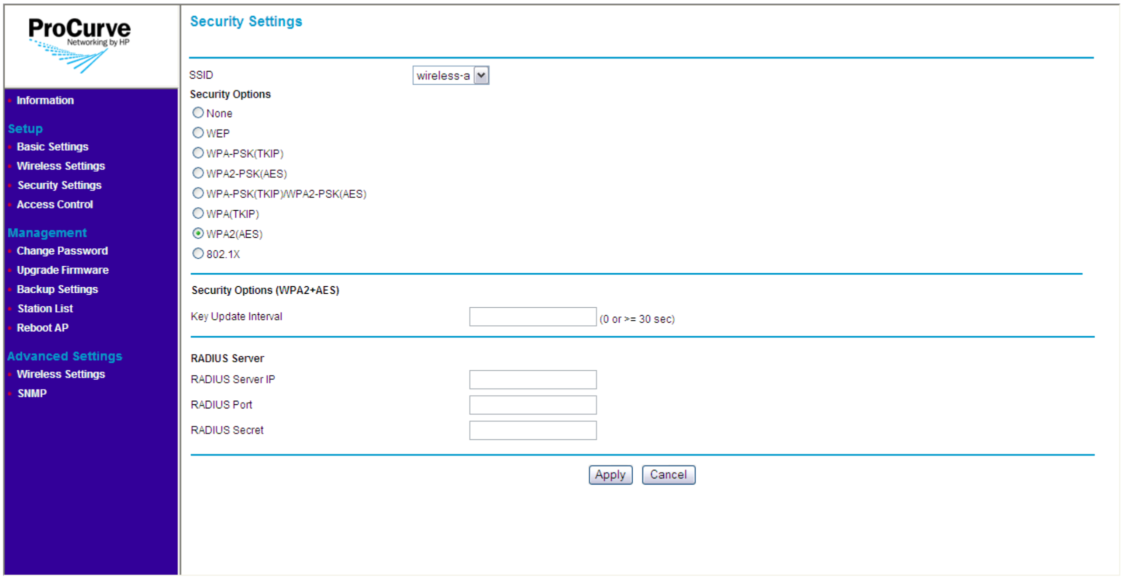
6. Click **Apply** to save your changes.

Repeat the same procedure for each SSID to which you want to assign WPA (TKIP) as its security profile.

Configuring WPA2 (AES)

This security profile uses AES as the encryption cipher and 802.1X as the authentication mechanism. In this way, each station is assigned a unique master key to derive the encryption between the access point and station, and the encryption keys can be automatically and periodically changed to further reduce the possibility of their discovery.

Figure 4-11. WPA2 (AES) Options



Security Settings

SSID: wireless-a

Security Options
○ None
○ WEP
○ WPA-PSK(TKIP)
○ WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
● WPA2(AES)
○ 802.1X

Security Options (WPA2+AES)
Key Update Interval: (0 or >= 30 sec)

RADIUS Server
RADIUS Server IP:
RADIUS Port:
RADIUS Secret:

To use WPA2 (AES):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. In the **Key Update Interval** box, define the time interval (in seconds) for regenerating a group key.
4. Under RADIUS Server, configure the RADIUS server settings:
   - **RADIUS Server IP**: Type the IP address of the RADIUS server on the network.
   - **RADIUS Port**: Type the User Datagram Protocol (UDP) port number used by the RADIUS server for accounting messages. Setting the port number to zero disables RADIUS authentication.

- **RADIUS Secret**: Type a shared text string used to encrypt messages between the access point and the RADIUS server. Make sure that the same text string is specified on the RADIUS Accounting server. Do not use blank spaces in the string. (Maximum length: 20 characters)

5. Click **Apply** to save your changes.

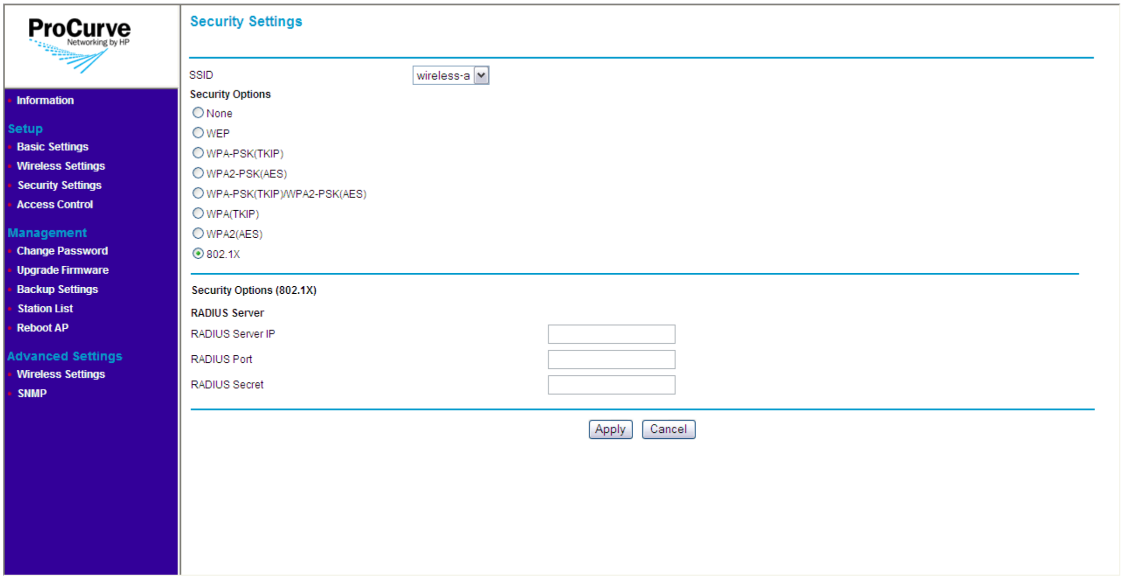
Repeat the same procedure for each SSID to which you want to assign WPA2 (AES) as its security profile.

Configuring 802.1X

802.1X is a standard frame-work for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication.

The 802.1X standard uses the Extensible Authentication Protocol(EAP) to pass user credentials (either digital certificates, usernames and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the access point grants client access to the network.

Figure 4-12. 802.1X Options



Security Settings

SSID: wireless-a

Security Options
○ None
○ WEP
○ WPA-PSK(TKIP)
○ WPA2-PSK(AES)
○ WPA-PSK(TKIP)/WPA2-PSK(AES)
○ WPA(TKIP)
○ WPA2(AES)
● 802.1X

Security Options (802.1X)

RADIUS Server

RADIUS Server IP

RADIUS Port

RADIUS Secret

To use 802.1X:

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **8021.x**.
4. Under Security Options (802.1X), configure the RADIUS server settings:
   - **RADIUS Server IP**: Type the IP address of the RADIUS server on the network.
   - **RADIUS Port**: Type the User Datagram Protocol (UDP) port number used by the RADIUS server for accounting messages. Setting the port number to zero disables RADIUS authentication.
   - **RADIUS Secret**: Type a shared text string used to encrypt messages between the access point and the RADIUS server. Make sure that the same text string is specified on the RADIUS Accounting server. Do not use blank spaces in the string. (Maximum length: 20 characters)
5. Click **Apply** to save your changes.

Repeat the same procedure for each SSID to which you want to assign 802.1X as its security profile.

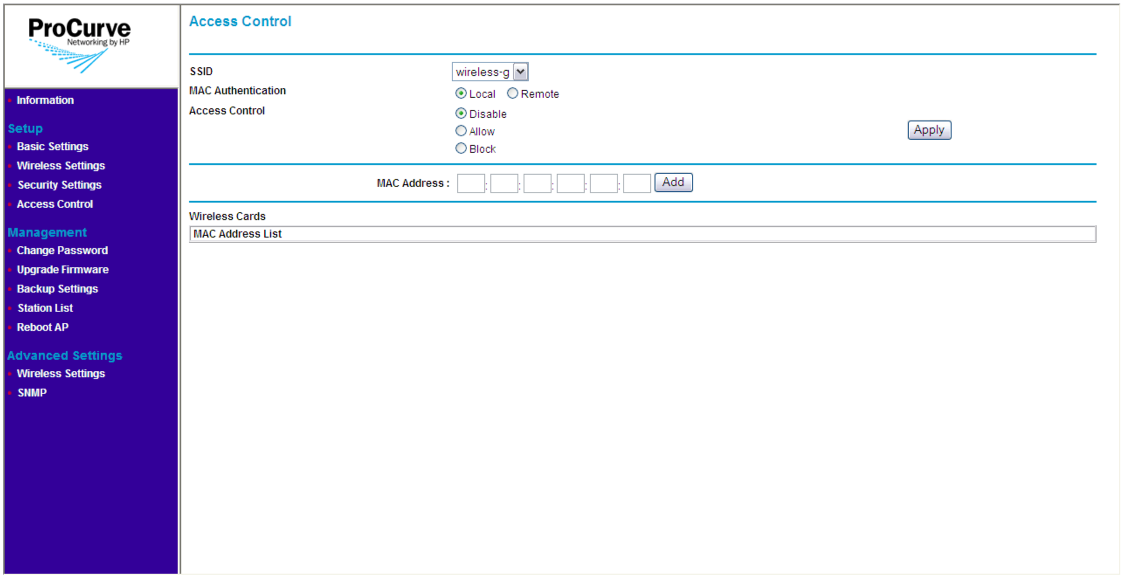
Controlling Access to the Wireless Network

You can configure the access point to authenticate client MAC addresses against a database stored locally on the access point or remotely on a RADIUS server. Client MAC addresses on the local database can be specified as allowed or blocked access the network. This enables the access point to control which devices can associate with the access point.

Note

Access control settings for each SSID/wireless interface need to be configured individually. Enabling access control for one SSID will not enable access control for the other.

Figure 4-13. Access Control Page



Access Control

SSID: wireless-g

MAC Authentication: ● Local ○ Remote

Access Control: ● Disable ○ Allow ○ Block

MAC Address : □ : □ : □ : □ : □ : □

Wireless Cards

MAC Address List

There are two options for setting up access control on the wireless network:

- Local MAC authentication, and
- Remote MAC authentication

Note

You can only use one type of MAC authentication at any given time. When both local and remote MAC authentication are enabled and configured, local MAC authentication will override remote MAC authentication.

Before setting up either type of MAC authentication, you will need to list down the MAC addresses of the wireless stations that you want to allow or block.

Setting Up Local MAC Authentication

Local MAC authentication allows you to add entries to the built-in MAC authentication database and to take certain actions based on a wireless client’s MAC address. The MAC list can be configured to allow or deny network access to specific clients.

Note

You can add up to 16 MAC addresses to the local MAC authentication database.

To configure local MAC authentication:

1. On the menu, click **Access Control**.
2. In **SSID**, select the SSID to which you want allow the wireless station access.
3. In **MAC Authentication**, select **Local**.
4. In **Access Control**, select the access option that you want to configure for the wireless station. Options include:
   - **Disable**: Click to disable MAC authentication. Selecting this option will disable *both* local and remote MAC authentication. After clicking **Disable**, click **Apply** to save your changes. You do not need to configure other settings.
   - **Allow**: Click to permit access to all MAC addresses except those listed on the local database as "block."
   - **Block**: Click to deny access to all MAC addresses except those listed on the local database as "allowed."
5. In the **MAC Address** box, enter the MAC or physical address of the wireless station that you want to allow or block. A MAC address consists of six pairs of alphanumeric characters, for example, 00 11 AA 22 BB 33.
6. Click **Add**. The page refreshes and the MAC address that you entered appears under **MAC Address List**.

   Repeat steps 5 to 6 for each wireless station that you want to allow or block.
7. Click **Apply**.

The message **Please wait...** appears as the address is added to the list. When the access point has completed the process, the MAC address appears in the MAC Address List table.

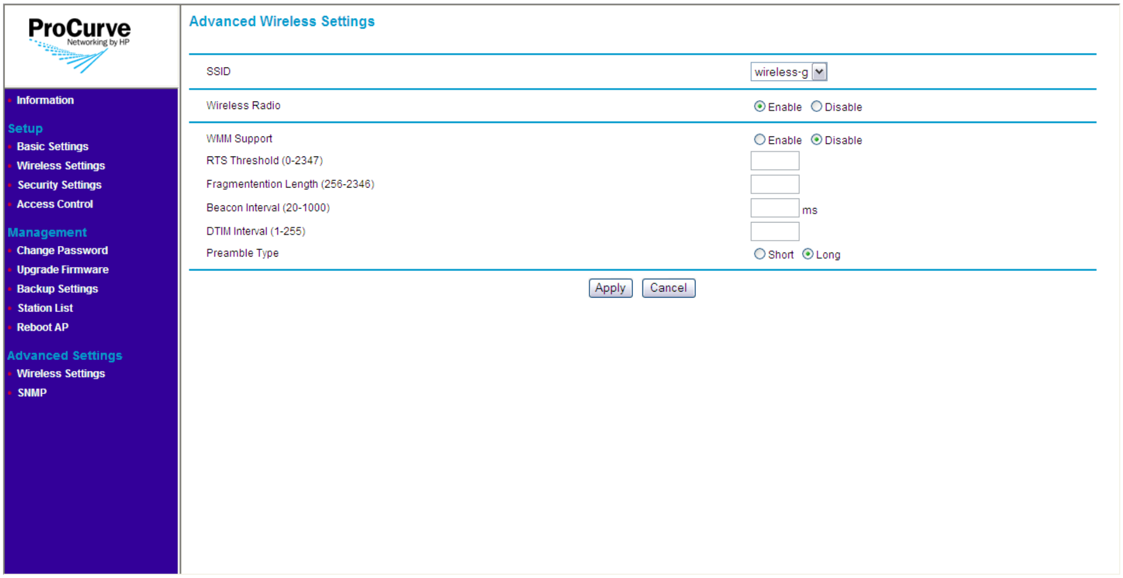
To delete a MAC address from the list, click the **Delete** button next to it.

Setting Up Remote MAC Authentication

Configuring Advanced Wireless Settings

Advanced wireless settings include options for enabling and disabling the wireless radios and Wi-Fi Multimedia (WMM). Options for fine tuning the access point's radio operation are also available.

Figure 4-14. Advanced Wireless Settings Page



Advanced Wireless Settings

SSID: wireless-g

Wireless Radio: ● Enable ○ Disable

WMM Support: ○ Enable ● Disable

RTS Threshold (0-2347)

Fragmentention Length (256-2346)

Beacon Interval (20-1000) ms

DTIM Interval (1-255)

Preamble Type: ○ Short ● Long

Apply Cancel

To configure the advanced wireless settings:

1. On the menu, click **Wireless Settings** under **Advanced Settings**.
2. In **SSID**, select the SSID for which you want configure the advanced wireless settings.
3. In **WMM Support**, click **Enable** if you want the access point to prioritize certain types of traffic above other traffic. When enabled, WiFi Multimedia (WMM) provides basic Quality of Service (QoS) to wireless network. HP recommends enabling this option if your network requires prioritization for voice or video traffic (for example, if network users use Voice over IP applications).

4. Configure the following advanced wireless settings for the SSID that you selected:
   - **RTS Threshold**: Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data. (Default is 2347)
   - **Fragmentation Length**: Configures the minimum packet size that can be fragmented when passing through the access point. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This speeds the retransmission of smaller frames. It is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. If set to 2346, this feature is disabled. Range: 256-2346, even numbers. (Default is 2346)
   - **Beacon Interval**: The rate at which beacon frames are transmitted from the access point. The beacon frames allow wireless stations to maintain contact with the access point. They may also carry power-management information. Range: 20-1000 ms (Default is 100)
   - **DTIM Interval**: The Delivery Traffic Indication Message (DTIM) interval helps keep marginal clients connected by sending "wake up" frames. Range: 1- 255 (Default is 1).
   - **Preamble Type:** Sets the length of the signal preamble used at the start of a data transmission. Using a short preamble can increase data throughput on the access point, but requires all associated stations be able to support a short preamble. (Default is Long)
     - **Long**: Sets the preamble to long. Using a long preamble ensures the access point can support all 802.11b and 802.11g stations
     - **Short**: Sets the preamble according to the capability of stations that are currently associated. Uses a short preamble if all associated stations can support it, otherwise a long preamble is used.
5. Click **Apply** to save your changes

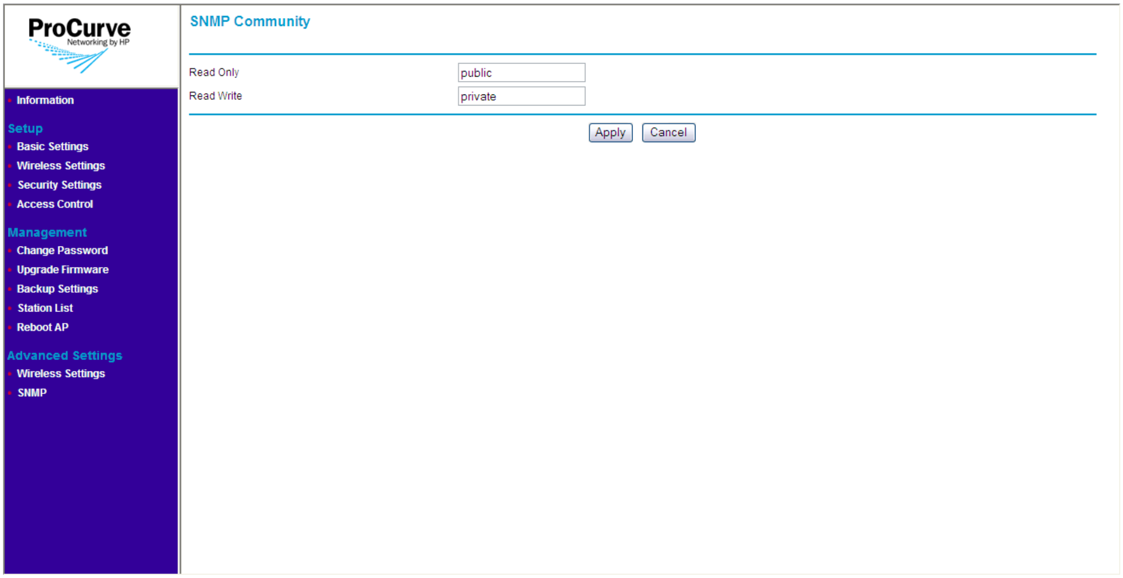
Setting the SNMP Community Names

You can manage the access point from a network management station running a Simple Network Management Protocol (SNMP) management application, such as ProCurve Manager.

The access point SNMP agent supports SNMP versions 1 and 2c. Management access from SNMP v1 or v2c stations is controlled by community names. To communicate with the access point, an SNMP v1 or v2c management station must first submit a valid community name for authentication.

The default community names are **public** for read-only access and **private** for read/write access. If you intend to support SNMP v1 or v2c managers, HP recommends that you change the default community names to prevent unauthorized access.

Figure 4-15. SNMP Community Page



SNMP Community

Read Only: public
Read Write: private

To change the default SNMP community names:

1. On the menu, click **SNMP**. The SNMP Community page appears.
2. To establish a public read-only SNMP community, type a **name** text string to replace the default community name (public) in the **Read Only** text field.

3. To establish a private read-write SNMP community, type a **name** text string to replace the default community name (private) in the **Read Write** text field.

4. Click **Apply** to save your changes and activate the new SNMP community names.

Supported MIB Browsers

In addition to ProCurve Manager, you can also use third-party management information base (MIB) browsers to manage the access point via SNMP. MIB browsers such as Net-Snmp management tool (version 5.1.2) and SNMPc Network Manager (version 7.0.18) are supported.

Managing the Access Point

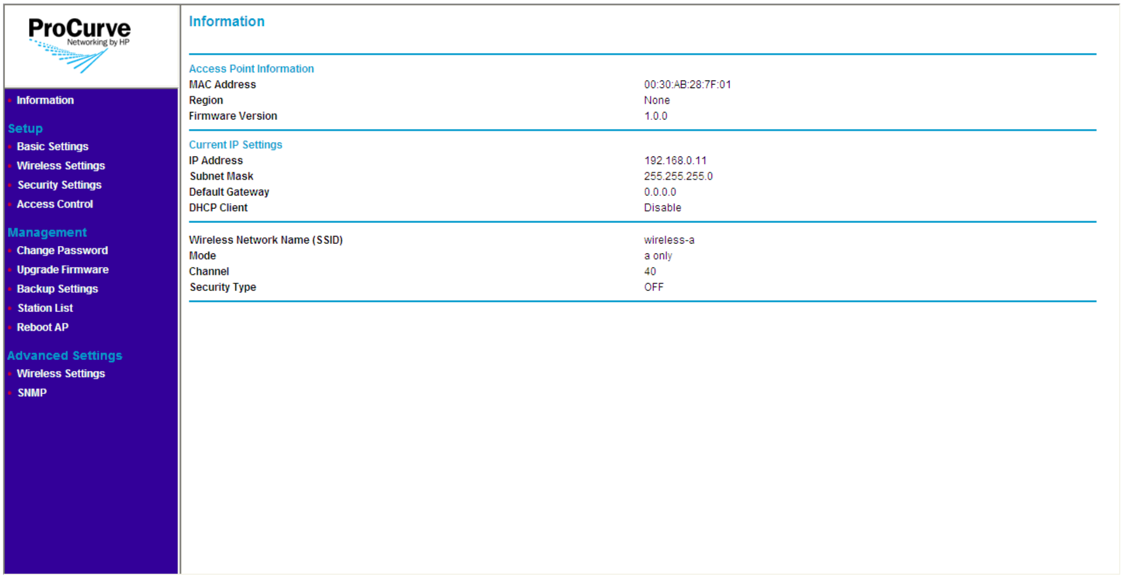
This chapter describes management tasks that you may periodically perform, including changing the management password and upgrading the firmware.

Topics discussed in this chapter include:

Viewing Device Information

Device information is available on the Information page, which is the default home page that loads after you log on to the Web interface. To access the Information page when you are already logged on, click **Information** on the menu.

Figure 5-1. Information Page



Information

Access Point Information	
MAC Address	00:30:AB:28:7F:01
Region	None
Firmware Version	1.0.0
Current IP Settings	
IP Address	192.168.0.11
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disable
Wireless Network Name (SSID)	wireless-a
Mode	a only
Channel	40
Security Type	OFF

The Information page displays three types of device information:

- Access Point Information
  - **MAC Address**: The physical layer address for the Ethernet port interface
  - **Region**: Shows the country/region that was set on the Basic Setting page
  - **Firmware Version**: Shows the version number for the runtime software
- Current IP Settings
  - **IP Address**: Shows the IP address of the management interface for this device
  - **Subnet Mask**: Shows the subnet mask configured for the management interface
  - **Default Gateway**: Show the IP address of the next-hop gateway node for network traffic that needs to be able to reach off-subnet destinations.Gateway address
  - **DHCP Client**: Shows whether the built-in DHCP client is Enabled or Disabled.
- Wireless Network Information
  - **Wireless Network Name (SSID)**: SSID configured for this wireless network

- **Mode**: Shows the wireless mode in use, either g/b (802.11gb) or a (802.11a)
- **Channel**: Shows the wireless channel on which the access point is broadcasting signal.
- **Security Type**: Shows the security profile assigned to this wireless interface.

Changing the Management Password

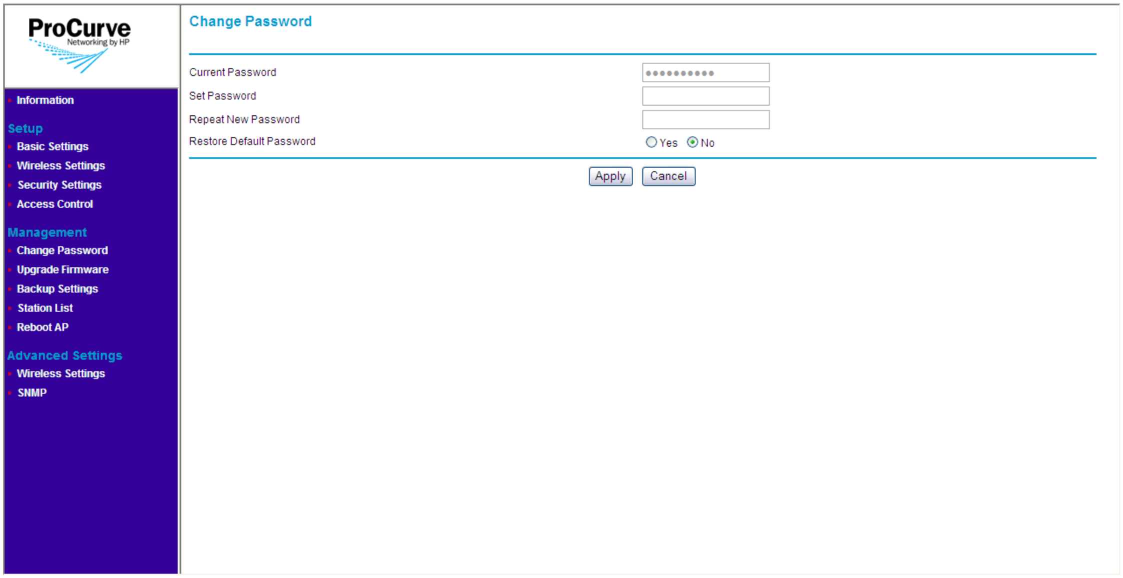
Management access to the Web interface is controlled through an administrator password. To prevent unauthorized users from accessing the Web interface and modifying the Access Point's settings, the interface is password-protected.

The default manager user name is **admin** and the default password is **password**.

Caution

HP strongly recommends that you change the default Web interface password *immediately* after your first logon. This will help prevent unauthorized users from logging on to the Web interface and changing the access point settings to compromise your network.

Figure 5-2. Change Password Page



Change Password

Current Password ●●●●●●●●●●

Set Password

Repeat New Password

Restore Default Password ○ Yes ● No

To change the default Web interface password:

1. On the menu, click **Change Password**. The Change Password page appears.
2. In **Set Password**, type your new password.

Note

The password is case-sensitive and must be between 1 and 32 alphanumeric characters long.

3. In **Repeat New Password**, type your new password again to confirm.
4. In **Restore Default Password**, click **No**.
5. Click **Apply** to save your changes.

Your new password is instantly applied, and the he logon dialog box appears after you save your new password. Enter your new password in the password box to log back into the Web interface.

If You Forget Your Password

If you lose the password, you can reset it by pressing the Reset to Default button on the back of the access point for one second to four seconds. This action resets the password to the default factory password, which is **password**.

Caution!

Do NOT press the Reset to Default button for more than four (4) seconds. Doing so will reset the access point to factory default configuration and erase all your current access point configuration.

Upgrading the Firmware

The upgrade function allows you to install on the Access Point any new firmware releases that may be made available. To install the new firmware, you first need to download the firmware from the HP Web site to the management computer.

Before performing an upgrade, take note of the current firmware version (shown on the Information page). You need to know this to be able to verify that the upgrade has been completed successfully.

Where to Download Firmware Upgrades

The ProCurve support site periodically provides access point software updates through the ProCurve Web site (http://www.procurve.com). Access point software updates are made available on the ProCurve Networking Web site, *http://www.hp.com/go/hpprocurve* under "**product support** > **software upgrades**."

For more information, see the support and warranty booklet shipped with the access point.

Upgrade Precautions

CAUTION!

Here are a few things that you can do to ensure that the upgrade process will be completed successfully:

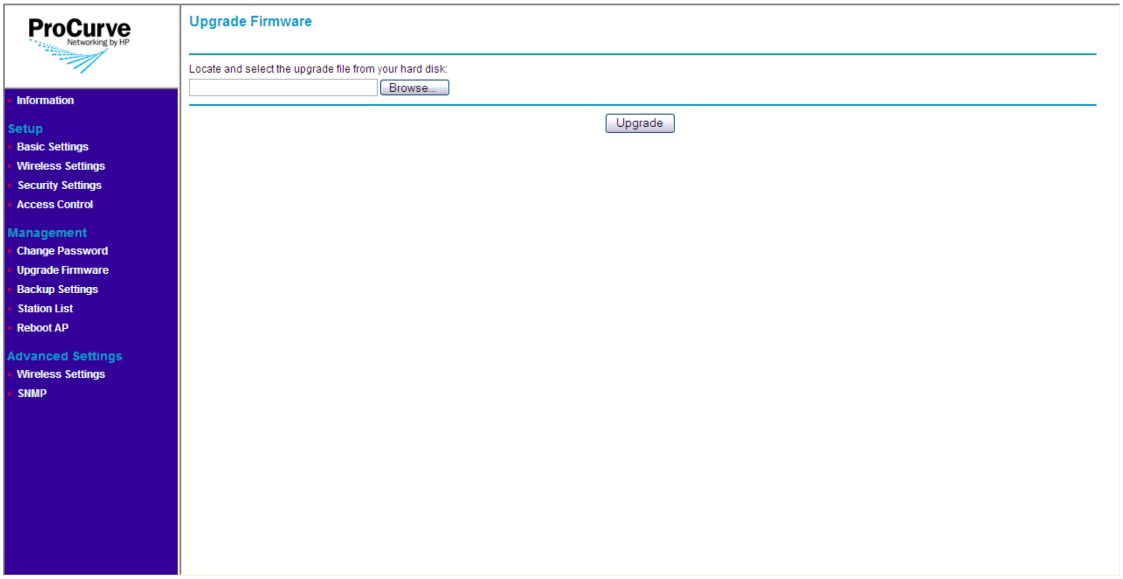
- Do not use your Web browser until the upgrade process has completed.
- Do not interrupt the Web browser by closing the window, clicking a link, or loading a new page.
- Do not interrupt the firmware upload by turning off your computer or the Access Point.

After an access point firmware update, the access point will automatically reboot and apply the updated code.

Note

Upgrading the firmware will not change the current configuration of the access point. The access point configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another access point of the same model. It is recommended that you save a copy of the configuration file before upgrading your access point software. See "Backing Up and Restoring Configuration" on page 5-8 for information on saving the access point's configuration file.

Figure 5-3. Upgrade Firmware Page



Locate and select the upgrade file from your hard disk:

Upgrade Procedure

To upgrade the access point firmware:

1. On the menu, click **Upgrade Firmware**. The Upgrade Firmware page appears.
2. Click **Browse**. The Choose File dialog box appears.
3. Go to the folder where you saved the upgrade file, select the file, and then click **Open**. The Choose File dialog box disappears.
4. Click **Upgrade**.

   When the firmware update is complete, the Access Point reboots itself, and then prompts you to log on to the Web interface again.
5. Log on to the Web interface.

6. On the menu, click **Information**.
7. Check the value for **Firmware Version** and verify that it shows a later version than what was installed before the update.

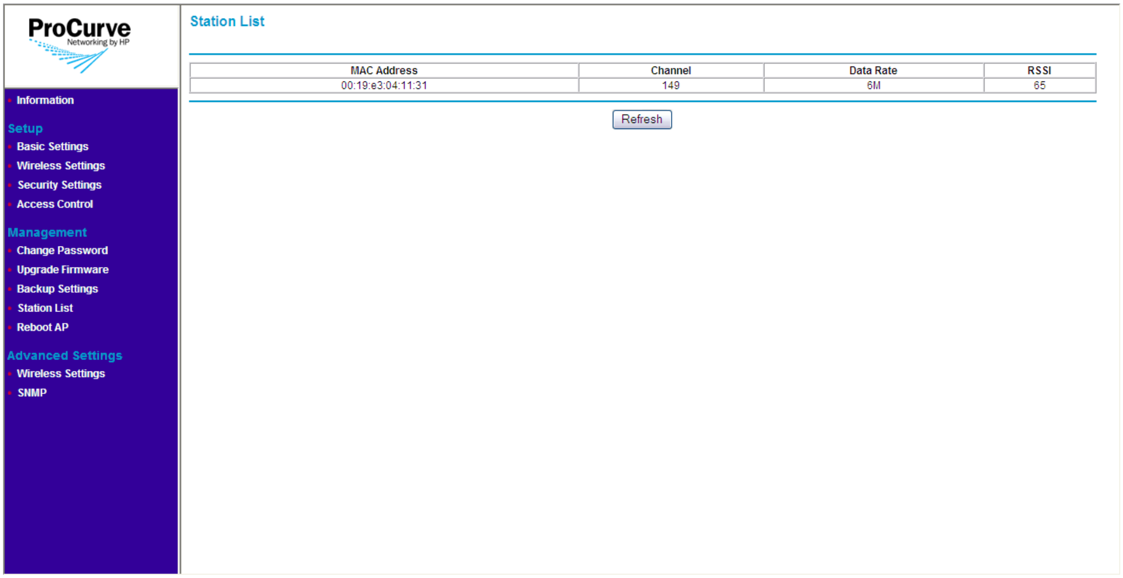
Viewing the List of Associated Stations

You can view which wireless stations are associated with the access point anytime by accessing the Station List page on the Web interface.

To access the page, click Station List on the menu. A table appears, which lists the following information about each associated wireless station:

- MAC address: Displays the MAC or physical address of the associated wireless station
- Channel: Displays the current channel on which the wireless station is receiving broadcast signal
- Data rate: Displays the transmission speed at which the wireless station is receiving data from the access point
- RSSI: Displays the received signal strength of the wireless station on the current wireless channel

Figure 5-4. Station List Page



Station List

MAC Address	Channel	Data Rate	RSSI
00:19:e3:04:11:31	149	6M	65

Backing Up and Restoring Configuration

To back up the current access point configuration:

1. On the menu, click **Backup Settings**. The Backup Settings page appears.
2. Click **Backup** under Save a Copy of Current Settings. A browser dialog box appears, as your browser attempts to download the configuration file from the access point.
3. Click **Save**. The Save As dialog box appears.
4. Choose a location where to save the configuration file and, if you want, change the file name. The default file name is `HP500_POE_R.cfg`. If you are changing the file name, HP recommends including the current date in the file name for ease of identification.
5. Click **Save**.
6. Start Windows Explorer, and then browse to the location where you save the configuration file, and then verify that it has been downloaded successfully.

To restore a backup configuration:

1. On the menu, click Backup Settings. The Backup Settings page appears.
2. Click **Browse** under Restore Saved Setting from a File.
3. When the Choose File dialog box appears, browse to the location where you saved the backup configuration file.
4. Select the backup file (default file name is `HP500_POE_R.cfg)`, and then click **Open**.
5. Click **Restore**. A confirmation message appears.

Caution!

Restoring settings from a backup configuration file will overwrite all current access point settings. Make sure you are restoring the correct backup file.

6. Click **OK** to restore settings from the backup file and overwrite the current settings. The message Please wait... appears as the access point restores the backup configuration file. When the access point has completed the restore process, the following message appears:

   AP is rebooting......

   PLEASE WAIT until re-directed to Information page.

The browser page refreshes, and the Information page appears.

Rebooting the Access Point

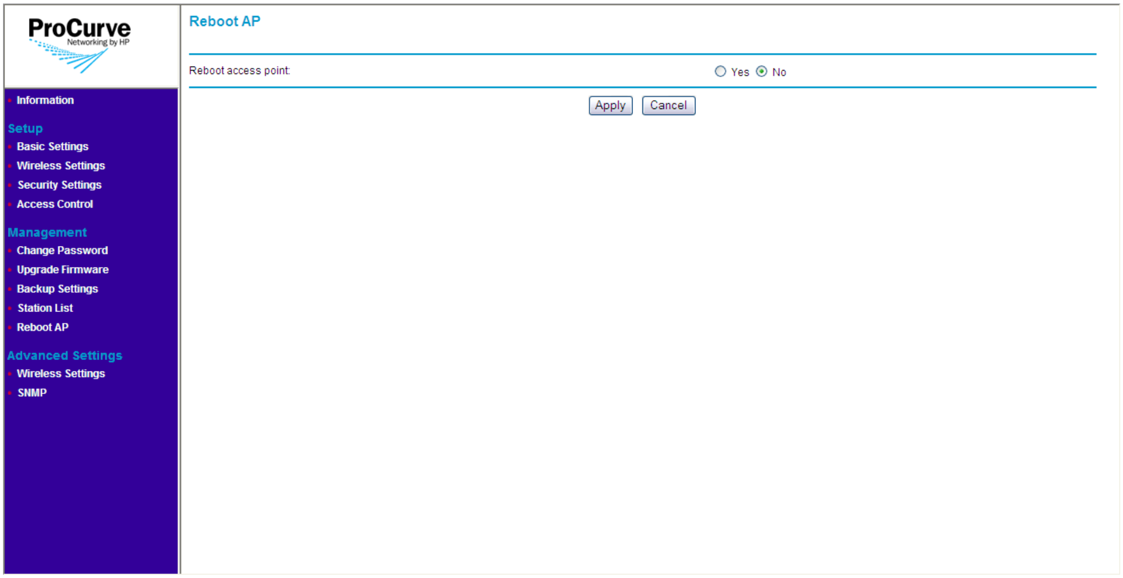
If you feel that the Access Point is not operating normally, try rebooting the device. This clears memory resources in use and can help restore normal operation.

Note that rebooting the Access Point will temporarily disconnect any wireless stations that are connected to it. If you have users on the network that are connected to the Internet through the Access Point, they will be temporarily disconnected. Their connection will be restored as soon as the Access Point has completed rebooting.

You can reboot the access point by pressing the Reset to Default button (on the rear of the access) for one to three seconds. Alternatively, you can click **Reboot AP** on the Web interface to perform the same action.

Refer to the procedure below for instructions on how to reboot the access point from the Web interface.

Figure 5-5. Reboot Page



Reboot AP

Reboot access point: ○ Yes ● No

To reboot the Access Point:

1. On the menu, click **Reboot AP**.
2. In **Reboot access point**, click **Yes**.
3. Click **Apply**. A confirmation message appears.
4. Click **OK**. The following message appears:

AP is rebooting......

PLEASE WAIT until re-directed to Information page.

When the Access Point has rebooted, the logon dialog box appears.

5. Enter your user name and password to log back on to the Web interface.

Troubleshooting

This chapter describes how to troubleshoot your ProCurve Wireless Access Point 10ag. Note that this document describes troubleshooting mostly from a hardware perspective.

This chapter describes the following:

Basic Troubleshooting Tips

Most problems are caused by the following situations. Check for these items first when starting your troubleshooting:

- **Connecting to devices that have a fixed full-duplex configuration.** By default, the RJ-45 port uses auto-negotiation to determine the duplex mode. That is, when connecting to attached devices, the access point will operate in one of two ways to determine the link speed and the communication mode (half duplex or full duplex):
  - If the connected device is also configured to use auto-negotiation, the access point will automatically negotiate both link speed and communication mode.
  - If the connected device has a fixed configuration, for example 100 Mbps, at half or full duplex, the access point will automatically sense the link speed, but will default to a communication mode of *half* duplex.

  Because the Access Point 10ag behaves in this way *(in compliance with the IEEE 802.3-2005 standard)*, if a device connected to the access point has a fixed configuration at *full* duplex, the device will not connect correctly to the access point. The result will be high error rates and very inefficient communications between the access point and the device.

All devices connected to the Access Point 10ag should be configured to auto-negotiate. To correct this problem you have to manually set the access point's RJ-45 port to match the duplex mode used by the attached device.

- **Faulty or loose cables.** Look for loose or obviously faulty connections. If the cables appear to be OK, make sure the connections are secure. If that does not correct the problem, try a different cable.
- **Non-standard cables.** Non-standard and miswired cables may cause network collisions and other network problems, and can seriously impair network performance. Use a new correctly-wired cable or compare your cable to the cable in appendix Appendix B, Access Point Port and Network Cables for pinouts and correct cable wiring. A category 5 cable tester is a recommended tool for every 100Base-TX network installation.
- **Improper network topologies.** It is important to make sure you have a valid network topology. Common topology faults include excessive cable length and excessive repeater delays between end nodes. If you have network problems after recent changes to the network, change back to the previous topology. If you no longer experience the problems, the new topology is probably at fault. Sample topologies are shown at the end of Chapter 2 in this book, and some topology configuration guidelines can be found online at the ProCurve Networking Web site,
  http://www.hp.com/rnd/index.htm
  under "network configuration examples."
- **Mobile users cannot connect to the network.** Make sure that the access point and wireless stations are configured with compatible security settings. Check to ensure that the wireless station is within the maximum range supported by the access point. Also verify that the wireless station has been configured with an IP address compatible with the attached network, either manually or via DHCP.

For more information on possible network problems and their solutions, refer to the technical note "Troubleshooting LAN Performance and Intermittent Connectivity Problems", which can be found on the ProCurve Networking Web site, *http://www.hp.com/go/hpprocurve*, in the Reference Library section under *http://www.hp.com/rnd/library/index.htm* under "T" in the "A-Z index."

Diagnosing with the LEDs

Table 6-1 shows LED patterns on the access point that indicate problem conditions.

1. Check in the table for the LED pattern that you see on your access point.
2. Refer to the corresponding diagnostic tip on the next few pages.

Table 6-1. LED Error Indicators

LED Pattern Indicating Problems			Diagnostic Tips
Power LED	**Radio LEDs**	**LAN LED**	
Off with power cord plugged in	*	*	**1**
Off without power cord plugged in, but linked to a PoE source	*	*	**2**
Prolonged on or off during initialization†	Prolonged on or off during initialization†	Prolonged on or off during initialization†	**3**
On	Off	*	**4**
On	*	Off with cable connected	**5**
On	*	On, but the port is not communicating	**6**

*** This LED is not important for the diagnosis.**
† Initialization takes between 30 seconds and one minute after a power on or reset.

Diagnostic Tips

Tip	Problem	Solution
1	The access point is not plugged into an active AC power source, or the access point's AC power adapter may have failed.	1. Verify that the power cord is plugged into an active power source and to the access point's AC power adapter. Make sure these connections are secure. 2. Try power-cycling the access point by unplugging and plugging the power cord back in. 3. If the Power LED is still not on, verify that the AC power source works by plugging another device into the outlet. Or try plugging the access point into a different outlet or try a different power cord. If the power source and power cord are OK and this condition persists, the access point's AC power adapter may have failed. Call your HP-authorized network reseller, or use the electronic support services from HP to get assistance. See the Customer Support/ Warranty booklet for more information.
2	The access point is not receiving power from the PoE source.	1. Verify that access point's 10/100Base-TX port is attached to a PoE source device. 2. Verify that the PoE source device is powered on, and that the PoE function has been administratively enabled on the source port attached to the access point. 3. Refer to Tip 6 to verify that the network cable is functioning properly.
3	The access point has experienced a software failure during initialization.	After a power on or reset, the LEDs indicate stages of the system initialization. If there is a software failure during initialization, the LED pattern indicates at which stage the failure occurred. The normal LED sequence during initialization is as follows: Stage 1. Power LED on for 5 seconds. System initialization has started. Stage 2. LAN LED blinks 5 times in 1 second. The boot ROM has successfully initialized. Stage 3. All LEDs on for 5 seconds. The operating system kernel has successfully loaded. Stage 4. LAN LED on only. The operating system is mounting the file system. Stage 5. LAN and 11a/b/g LEDs on. Radio drivers have been successfully loaded. Stage 6. LAN, 11a/b/g, and 11b/g LEDs on. The access point software is initializing. Stage 7. Normal LED operation. Initialization has completed successfully. The entire initialization sequence takes between 30 seconds (normal reset) and one minute (factory default reset). If one of the above LED patterns display longer than one minute, a failure has occurred. Do the following: 1. Reset the access point by pressing the Reset button on the back of the access point, or by power cycling the access point. 2. If the fault indication reoccurs, take note of the LED pattern and contact your HP-authorized network reseller, or use the electronic support services from HP to get assistance. See the Customer Support/Warranty booklet for more information.
4	Wireless link has been administratively disabled.	Verify that the wireless port has not been disabled through an access point configuration change. You can use the Web browser interface to determine the state of the wireless port and re-enable the port if necessary. Also verify that the country code has been set.

Tip	Problem	Solution
5	The 10/100Base-TX network connection is not working properly.	Try the following procedures: • Verify that both ends of the cabling, at the access point and the connected device, are connected properly. • Verify the connected device and access point are both powered *on* and operating correctly. • Verify duplex operation (see page 6-1). • If these procedures don’t resolve the problem, try using a different cable.

Hardware Diagnostic Tests

Testing the Access Point by Resetting It

If you believe that the access point is not operating correctly, you can reset the access point. To reset the access point, either

- Unplug and plug in the power cord (power-cycling).
- Press the Reset button on the back of the access point for about two seconds (until the LEDs start to blink rapidly).

Caution

If you press the Reset to Default button for five seconds or more, you will reset the board and reload the factory default settings. See "Restoring Factory Default Configuration" on page 6-7.

Power-cycling the access point and pressing the Reset to Default button both cause the access point to perform its system initialization, which normally resolves any temporary operational problems.

Checking the Access Point's LEDs

The system initialization is successful when the Power LED is on and the other LEDs are in a normal operating state after approximately one minute. If the LED pattern is different that this for longer than one minute, there may be a problem with the access point.

See "Diagnosing with the LEDs" on page 6-3 for information on interpreting the LED patterns.

Testing Twisted-Pair Cabling

Network cables that fail to provide a link or provide an unreliable link between the access point and the connected network device may not be compatible with the IEEE 802.3 Type 10Base-T, or 100Base-TX standards. The twisted-pair cables attached to the Access Point 10ag must be compatible with the appropriate standards. To verify that your cable is compatible with these standards, use a qualified cable test device.

Testing Access Point-to-Device Network Communications

You can perform the following communication tests to verify that the network is operating correctly between the access point and any connected device that can respond correctly to the communication test.

- Ping Test – a network layer test used on IP networks that sends test packets to any device identified by its IP address

Testing End-to-End Network Communications

Both the access point and the cabling can be tested by running an end-to-end communications test – a test that sends known data from one network device to another through the access point. You can run a PING test to verify that the entire communication path between the two network devices is functioning correctly.

Restoring Factory Default Configuration

As part of your troubleshooting process on the Access Point 10ag, it may become necessary to return the access point's configuration to its factory default settings. This process momentarily interrupts the access point's operation and reboots the access point. When restoring the factory default configuration, all settings are cleared, including the Manager password and any IP address.

Note

Restoring factory defaults removes all access point configuration changes that you have made from the factory default settings. This includes, for example, IP addresses, and radio interface settings. Returning the configuration of these features to their factory default settings may result in network connectivity issues.

If the access point has a valid configuration, and you are restoring the factory default settings for a reason other than configuration problems, you should save the access point configuration prior to performing the factory default reset. Then, after the reset and resolution of the original problem, you can restore the saved configuration to the access point.

You can restore factory default configuration either by pressing the Reset to Default button on the rear panel, or by clicking the **Erase** button on the Backup Settings page.

Note The system, password, custom default, and factory default reset functions can be disabled by the access point's software.

To restore to factory default using the Reset to Default button:

1. Using a pointed object such as the tip of a ballpoint pen or a straightened clip, press the Reset to Default button for five seconds or more. The LEDs flash rapidly (about 10 times per second).
2. As soon as the LEDs (except the Power LED) shut off, release the Reset to Default button.

The AP resets to factory defaults and reboots. You can then release the reset button.

To restore to factory default from the Web interface:

1. Log on to the Web interface.
2. On the menu, click **Backup Settings**. The Backup Settings page appears.

Caution! No warning or confirmation appears after you click **Erase**. The access point will restore its settings to factory default immediately.

3. Under Revert to Factory Default Settings, click **Erase**.

The following message appears:

Please wait....
AP is rebooting......
PLEASE WAIT until re-directed to Information page.

When the access point has completed restoring its settings to factory default, the Web interface refreshes and displays the Information page. If the access point was using an IP address other than the default, you may see a Page Not Found message in your browser. This is because the access point has already reverted to its default IP address, **192.168.1.11**, which may be incompatible with your current network settings.

HP Customer Support Services

If you are still having trouble with your access point, Hewlett-Packard offers support 24 hours a day, seven days a week through the use of a number of automated electronic services. See the Customer Support/Warranty booklet that came with your access point for information on how to use these services to get technical support. The ProCurve Networking Web site, *http://www.hp.com/go/hpprocurve* also provides up-to-date support information under "product support."

Additionally, your HP-authorized network reseller can provide you with assistance, both with services that they offer and with services offered by HP.

Before Calling Support

To make the support process most efficient, before calling your networking dealer or HP Support, you first should retrieve the following information:

Information Item	Information Location
• product identification	the front of the access point, Access Point 10ag (J9140A or J9141A)
• details about the access point's status including the firmware version and a copy of the access point configuration	• Web interface: Information page
• copy of your network topology map, including network addresses assigned to the relevant devices	your network records

— This page is intentionally unused. —

Specifications

Physical

Width:	178 mm
Depth:	103 mm
Height:	34 mm
Weight:	285 g

Electrical

Adapter

AC voltage:	100-240 volts, 0.5A, 50/60 Hz
DC voltage:	12 volts, 1.25A (max)
Power consumption:	15 watts (max)

Note: Power can also be provided to the access point through the Ethernet port based on IEEE 802.3af Power over Ethernet (PoE) specifications. The access point is a Class 3 device, that is, the maximum power required is in the range of 6.49 to 12.95 watts. When both PoE is provided and the adapter is plugged in, PoE is turned off.

Environmental

	Operating	**Non-Operating**
Temperature:	0°C to 40°C (32°F to 104°F) PoE mode	-40°C to 70°C (-40°F to 158°F)
Relative humidity: (non-condensing)	15% to 95%	10% to 90%
Maximum altitude:	3.05 Km (10,000 ft)	

Connectors

- The 10/100 Mbps RJ-45 twisted-pair port is compatible with the IEEE 802.3u 100Base-TX and IEEE 802.3 Type 10Base-T standards.

  Note: To provide Power over Ethernet to the access point, all 4 pairs of wires must be connected for any network cable attached to this port.

Safety

Complies with:

- IEC 60950-1: 2001
- EN 60950-1: 2002
- UL 60950-1 1st Ed.
- CAN/CSA-C22.2 No. 60950-1-03

EMC Compliance (Class B)

Complies with:

- FCC Part 15.107 and 15.109
- ICES-003 (Canada)
- VCCI

Radio Signal Certification

Complies with:

- FCC Part 15, Subpart C and E
- RSS-210 (Canada), Issue 7 (June 2007)
- EN300.328 v1.7.1 (2006-10)
- EN 301.893 V1.2.3 (2003-08)
- ARIB RCR STD-T66 (Ch 1~13), STD-33 (Ch 14), STD-71 (802.11a)
- DGT LP0002 (Taiwan)

Immunity

- EN 301.489-1 v1.6.1 (2005-09)
- EN 301.489-17 V1.2.1 (2002-08)
- EN 60601-1-2

Wireless

802.11b/g

Radio Standard:	IEEE 802.11b/g
Radio Technology:	Direct Sequence Spread Spectrum (DSSS) Orthogonal Frequency Division Multiplexing (OFDM)
Data Rate:	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
Operating Frequency:	2.4 ~ 2.4835 GHz (US, Canada, Taiwan, ETSI) 2.4 ~ 2.497 GHz (Japan)
Maximum Channels:	FCC/IC/NCC: 1-11, ETSI: 1-13, MKK: 1-13 (802.11g), 1-14 (802.11b)
Modulation Type:	BPSK, QPSK, 16QAM, 64QAM / OFDM, BPSK, QPSK, CCK / DSSS
Media Access Protocol:	CSMA/CA with ACK
Transmit Output Power:	18 dBm (max)

802.11a

Radio Standard:	IEEE 802.11a
Radio Technology:	Orthogonal Frequency Division Multiplexing (OFDM)
Data Rate:	6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel
Operating Frequency:	5.15 ~ 5.25 GHz (lower band) US, Canada, Japan, ETSI 5.25 ~ 5.35 GHz (middle band) Taiwan, Japan, ETSI 5.725~5.85 GHz (upper band) US, Canada, Taiwan 5.47 ~ 5.725 GHz ETSI
Maximum Channels:	FCC/IC/NCC: 9, ETSI: 19, MKK: 8
Modulation Type:	BPSK, QPSK, 16QAM, 64QAM
Media Access Protocol:	CSMA/CA with ACK
Transmit Output Power:	18 dBm (max)

Antenna Type and Gain

Antenna Type:	Dipole
Antenna Gain:	2.4GHz ~ 2.5GHz 1.78 (dBi) 5.15GHz ~ 5.25GHz 1.65 (dBi) FCC/IC/MKK/ETSI 5.25GHz ~ 5.35GHz 1.4 (dBi) ETIS/ECC/MKK 5.470GHz ~ 5.725GHz 2.28 (dBi) ETSI 5.725GHz ~ 5.85GHz 1.78 (dBi) FCC/IC/NCC

Receiver Sensitivity

Radio	ProCurve AP 10ag NA (J9140A)	ProCurve AP 10ag (J9141A)
802.11b (typical)	11Mbps @ -87dBm; 5.5Mbps @ -91dBm; 2Mbps @ -92dBm; 1Mbps @ -97dBm	11Mbps @ -87dBm; 5.5Mbps @ -89dBm; 2Mbps @ -91dBm; 1Mbps @ -94dBm
802.11g (typical)	54Mbps @ -74dBm; 48Mbps @ -75dBm; 36Mbps @-80dBm; 24Mbps @ -83dBm; 18Mbps @-86dBm; 12Mbps @ -88dBm; 9Mbps @ -90dBm; 6Mbps @ -91dBm	54Mbps @ -75dBm; 48Mbps @ -77dBm; 36Mbps @ -81dBm; 24Mbps @ -84dBm; 18Mbps @-87dBm; 12Mbps @ -88dBm; 9Mbps @ -89dBm; 6Mbps @ -90dBm
802.11a (typical)	54Mbps @ -70dBm; 48Mbps @ -72dBm; 36Mbps @-78dBm; 24Mbps @ -81dBm; 18Mbps @-85dBm; 12Mbps @ -87dBm; 9Mbps @ -89dBm; 6Mbps @ -90dBm	54Mbps @ -70dBm; 48Mbps @ -72dBm; 36Mbps @-78dBm; 24Mbps @ -81dBm; 18Mbps @-84dBm; 12Mbps @ -87dBm; 9Mbps @ -88dBm; 6Mbps @ -89dBm

B

Access Point Port and Network Cables

This appendix includes access point connector information and network cable information for cables that should be used with the Access Point 10ag, including minimum pin-out information and specifications for twisted-pair cables.

Note

Incorrectly wired cabling is the most common cause of problems for LAN communications. HP recommends that you work with a qualified LAN cable installer for assistance with your cabling requirements.

Access Point Ports

The fixed RJ-45 10/100Base-TX port on the access point accepts 100-ohm unshielded twisted-pair cable with RJ-45 connectors as described on the next page.

Twisted-Pair Cables

10 Mbps Operation	Category 5 100-ohm unshielded twisted-pair (UTP), complying with IEEE 802.3 Type 10Base-T specifications, fitted with RJ-45 connectors
100 Mbps Operation	Category 5 100-ohm UTP cable, complying with IEEE 802.3u 100Base-TX specifications, fitted with RJ-45 connectors

Twisted-Pair Cable/Connector Pin-Outs

The access point includes one 10/100Base-TX port. This port uses the “HP Auto MDIX” feature, which means that you can use either straight-through or crossover twisted-pair cables to connect the access point to a switch.

Other Wiring Rules:

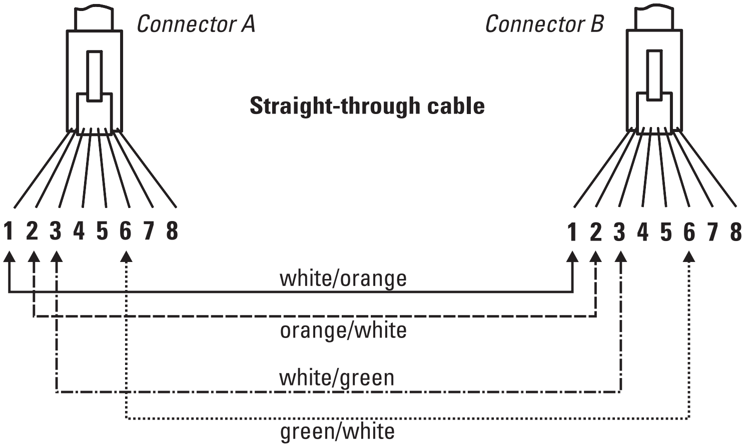
- All twisted-pair wires used for 10 Mbps, and 100 Mbps operation must be twisted through the entire length of the cable. The wiring sequence must conform to EIA/TIA 568-B (not USOC). See “Twisted-Pair Cable Pin Assignments” later in this appendix for a listing of the signals used on each pin.
- For 10 Mbps connections to the ports, you can use Category 5 unshielded twisted-pair cable, as supported by the IEEE 802.3 Type 10Base-T standard.
- For 100 Mbps connections to the ports, use 100-ohm Category 5 UTP cable only, as supported by the IEEE 802.3u Type 100Base-TX standard.
- To provide Power over Ethernet to the access point, all 4 pairs must be connected for any network cable attached to this port; the cable must meet ISO/DIS 11801 Class D requirements and IEEE 802.3af requirements.

Access Point Port and Network Cables

Straight-Through Twisted-Pair Cable for 10 Mbps or 100 Mbps Network Connections

Because the 10/100 port on the access point supports auto-MDIX operation, you can use either "straight-through" or "crossover" cable for network connections to PCs, servers, hubs, or switches.

Cable Diagram



Note

Pins 1 and 2 on connector "A" *must* be wired as a twisted pair to pins 1 and 2 on connector "B".
Pins 3 and 6 on connector "A" *must* be wired as a twisted pair to pins 3 and 6 on connector "B".
Pins 4, 5, 7, and 8 are not used for transmitting or receiving data, although they must be wired straight-through in the cable to support Power over Ethernet.

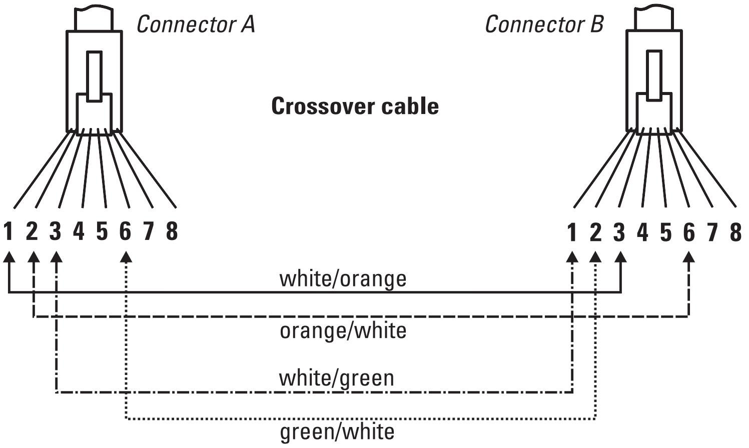
Pin Assignments

Access Point End (MDI)			**Hub or Switch Port, or Other MDI-X Port End**	
Signal	**Pins**		**Pins**	**Signal**
receive +	1	◄──────	1	transmit +
receive -	2	◄──────	2	transmit -
transmit +	3	──────►	3	receive +
transmit -	6	──────►	6	receive -

Crossover Twisted-Pair Cable for 10 Mbps or 100 Mbps Network Connection

Because the 10/100 port on the access point supports auto-MDIX operation, you can use either “straight-through” or “crossover” cable for network connections to PCs, servers, hubs, or switches.

Cable Diagram



Note

Pins 1 and 2 on connector “A” *must* be wired as a twisted pair to pins 3 and 6 on connector “B”.
Pins 3 and 6 on connector “A” *must* be wired as a twisted pair to pins 1 and 2 on connector “B”.
Pins 4, 5, 7, and 8 are not used for transmitting or receiving data, although they must be wired straight-through in the cable to support Power over Ethernet.

Pin Assignments

Access Point End (MDI)		**Computer, Transceiver, or Other MDI Port End**	
Signal	**Pins**	**Pins**	**Signal**
receive +	1 ←	6	transmit -
receive -	2 ←	3	transmit +
transmit +	3 →	2	receive -
transmit -	6 →	1	receive +

C

Safety and EMC Regulatory Statements

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 the equipment or create a non-compliant condition.

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

Grounding

This product is a safety class I compliant product and has a protective earthing terminal. There must be an uninterruptible safety earth ground from the main power source to the product's 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.

Servicing

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

This product does not have a power switch; it is powered on when the power cord is plugged in.

Regulatory Model Identification Number

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is RSVLC-0702. The RMN should not be confused with the marketing name (ProCurve Wireless Access Point 10ag) or the Product Numbers J9140A (NA) and J9141A (WW).

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.

Cet appareil ne comporte pas de commutateur principal ; la mise sous tension est effectuée par branchement du cordon d'alimentation.

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 Eine WARNING in der Dokumentation symbolisiert eine Gefahr, die Verletzungen oder sogar Todesfälle verursachen kann.

CAUTION CAUTION in der Dokumentation symbolisiert eine Gefahr, die dis Gerät beschädigen kann.

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.

Dieses Gerät hat keinen Netzschalter; es wird beim Anschließen des Netzkabels eingeschaltet.

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 WARNING denota un pericolo che può causare lesioni o morte.

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

Non procedere oltre un avviso di WARNING o di CAUTION prima 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.

Questo apparato non possiede un commutatore principale; si mette scotto tensione all'inserirsi il cavo d'alimentazione.

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.

Este producto no tiene interruptor de potencia; se activa cuando se enchufa el cable de alimentación.

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。

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。

安装

安装辅助管理模块，请参看安装指南。

保修及技术支持

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，请按以下 方式与我们联络。

如是硬件故障:

1. 与售出单位或当地维修机构联系。
2. 中国惠普有限公司维修中心地址:
   北京市海淀区知春路49号希格玛大厦
   联系电话: 010-62623888 转 6101
   邮政编码: 100080

如是软件问题:

1. 惠普用户响应中心热线电话: 010-65645959
2. 传真自动回复系统: 010-65645735

EMC Regulatory Statements

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

We declare that the product is limited in CH1-CH11 for 2.4G band by specific firmware controlled by the manufacturer and is not user changeable.

IC Statement

Operation is subject to the following two conditions:

1) This device may not cause interference and

2) This device must accept any interference, including interference that may cause undesired operation of the device.

IMPORTANT NOTE: IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

(i) the device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems;

(ii) the maximum antenna gain permitted (for devices in the bands 5250-5350 MHz and 5470-5725 MHz) to comply with the e.i.r.p. limit; and

(iii) the maximum antenna gain permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

In addition, users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/ or damage to LE-LAN devices.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

1) Ce périphérique ne doit pas causer d'interférence et.

2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

NCC Statement

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

工作頻率5.250~5.350GHz該頻段限於室內使用

Telec Label

CE Statement

Europe - EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN 60 950-1: 2001 +A11: 2004
Safety of Information Technology Equipment

EN50385 : (2002-08)
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 301 893 V1.2.3: (2003-08)
Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

EN 300 328 V1.7.1 (2006-10)
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.6.1: (2005-09)
Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electro-Magnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V1.2.1 (2002-08)
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electro-Magnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France

CE (!)

Česky [Czech]	[Jméno výrobce] tímto prohlašuje, že tento [typ zařízení] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklćrer herved, at fřlgende udstyr *[udstyrets typebetegnelse]* overholder de vćsentlige krav og řvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ pőhinőuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Espańol [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* č conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguęs [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* stĺr I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgĺr av direktiv 1999/5/EG.

Open Source Licenses

Contents

Overview

This appendix includes the following information:

- Open Source licenses

GPL2 (GNU General Public License, v.2)

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have

received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>Copyright (C) 19yy <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.
>
> <signature of Ty Coon>, 1 April 1989Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GPL + Linking Exception

“GPL2 (GNU General Public License, v.2)” plus an exception permitting linking the library with other software.

ClearSilver

Neotonic ClearSilver is available under the following license, derived from the Apache Software License v1.1

For alternative licensing, please contact the authors at clearsilver@neotonic.com Neotonic ClearSilver Software License

Version 1.0

Copyright (c) 2001 Brandon Long and Neotonic Software Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

> "This product includes software developed by the Neotonic Software Corporation. (http://www.neotonic.com/)."
>
> Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4.The names "Neotonic" and "Neotonic ClearSilver" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact clearsilver@neotonic.com.

5.Products derived from this software may not be called "ClearSilver", nor may "ClearSilver" appear in their name, without prior written permission of Neotonic Software Corporation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NEOTONIC, INC., OR ITS CLEARSILVER CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of Neotonic Software Corporation. For more information on Neotonic Software Corporation, please see http://www.neotonic.com/.

Some of the concepts of this software are based on previous software developed by Scott Shambarger, Paul Clegg, and John Cwikla. The current authors wish to thank them for their efforts.

Dropbear License

The majority of code is written by Matt Johnston, under the following license:

=====

LibTomCrypt and LibTomMath are (c) Tom St Denis, under TDCAL (Tom Doesn't Care About Licenses) some files are from public domain sources, see libtomcrypt/legal.txt

=====

sshpty.c is taken from OpenSSH 3.5p1,

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed

under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS.

LGPL (GNU Lesser General Public License)

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offerwarranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

> a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the library's name and a brief idea of what it does.>Copyright (C) <year> <name of author>
>
> This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.
>
> <signature of Ty Coon>, 1 April 1990Ty Coon, President of Vice

That's all there is to it!

Intel (2)

MIT

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

> This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CMU (Carnegie Mellon University)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

> Office of Technology Transfer
>
> Carnegie Mellon University
>
> 5000 Forbes Avenue
>
> Pittsburgh, PA 15213-3890
>
> (412) 268-4387, fax: (412) 268-7395
>
> tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

> "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSSL

LICENSE ISSUES

===============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

===

Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4.The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5.Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6.Redistributions of any form whatsoever must retain the following acknowledgment:"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

===
==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement::

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Recycle Statements

Waste Electrical and Electronic Equipment (WEEE) Statements

Disposal of Waste Equipment by Users in Private Household in the European Union

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Likvidace zařízení soukromými domácími uživateli v Evropské unii

Tento symbol na produktu nebo balení označuje výrobek, který nesmí být vyhozen spolu s ostatním domácím odpadem. Povinností uživatele je předat takto označený odpad na předem určené sběrné místo pro recyklaci elektrických a elektronických zařízení. Okamžité třídění a recyklace odpadu pomůže uchovat přírodní prostředí a zajistí takový způsob recyklace, který ochrání zdraví a životní prostředí člověka. Další informace o možnostech odevzdání odpadu k recyklaci získáte na příslušném obecním nebo městském úřadě, od firmy zabývající se sběrem a svozem odpadu nebo v obchodě, kde jste produkt zakoupili.

Bortskaffelse af affald fra husstande i den Europæiske Union

Hvis produktet eller dets emballage er forsynet med dette symbol, angiver det, at produktet ikke må bortskaffes med andet almindeligt husholdningsaffald. I stedet er det dit ansvar at bortskaffe kasseret udstyr ved at aflevere det på den kommunale genbrugsstation, der forestår genvinding af kasseret elektrisk og elektronisk udstyr. Den centrale modtagelse og genvinding af kasseret udstyr i forbindelse med bortskaffelsen bidrager til bevarelse af naturlige ressourcer og sikrer, at udstyret genvindes på en måde, der beskytter både mennesker og miljø. Yderligere oplysninger om, hvor du kan aflevere kasseret udstyr til genvinding, kan du få hos kommunen, den lokale genbrugsstation eller i den butik, hvor du købte produktet.

Seadmete jäätmete kõrvaldamine eramajapidamistes Euroopa Liidus

See tootel või selle pakendil olev sümbol näitab, et kõnealust toodet ei tohi koos teiste majapidamisjäätmetega kõrvaldada. Teie kohus on oma seadmete jäätmed kõrvaldada, viies need elektri- ja elektroonikaseadmete jäätmete ringlussevõtmiseks selleks ettenähtud kogumispunkti. Seadmete jäätmete eraldi kogumine ja ringlussevõtmine kõrvaldamise ajal aitab kaitsta loodusvarasid ning tagada, et ringlussevõtmine toimub viisil, mis kaitseb inimeste tervist ning keskkonda. Lisateabe saamiseks selle kohta, kuhu oma seadmete jäätmed ringlussevõtmiseks viia, võtke palun ühendust oma kohaliku linnakantselei, majapidamisjäätmete kõrvaldamise teenistuse või kauplusega, kust Te toote ostsite.

Laitteiden hävittäminen kotitalouksissa Euroopan unionin alueella

Jos tuotteessa tai sen pakkauksessa on tämä merkki, tuotetta ei saa hävittää kotitalousjätteiden mukana. Tällöin hävitettävä laite on toimitettava sähkölaitteiden ja elektronisten laitteiden kierrätyspisteeseen. Hävitettävien laitteiden erillinen käsittely ja kierrätys auttavat säästämään luonnonvaroja ja varmistamaan, että laite kierrätetään tavalla, joka estää terveyshaitat ja suojelee luontoa. Lisätietoja paikoista, joihin hävitettävät laitteet voi toimittaa kierrätettäväksi, saa ottamalla yhteyttä jätehuoltoon tai liikkeeseen, josta tuote on ostettu.

Élimination des appareils mis au rebut par les ménages dans l'Union européenne

Le symbole apposé sur ce produit ou sur son emballage indique que ce produit ne doit pas être jeté avec les déchets ménagers ordinaires. Il est de votre responsabilité de mettre au rebut vos appareils en les déposant dans les centres de collecte publique désignés pour le recyclage des équipements électriques et électroniques.   La collecte et le recyclage de vos appareils mis au rebut indépendamment du reste des déchets contribue à la préservation des ressources naturelles et garantit que ces appareils seront recyclés dans le respect de la santé humaine et de l'environnement. Pour obtenir plus d'informations sur les centres de collecte et de recyclage des appareils mis au rebut, veuillez contacter les autorités locales de votre région, les services de collecte des ordures ménagères ou le magasin dans lequel vous avez acheté ce produit.

Entsorgung von Altgeräten aus privaten Haushalten in der EU

Das Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass das Produkt nicht über den normalen Hausmüll entsorgt werden darf. Benutzer sind verpflichtet, die Altgeräte an einer Rücknahmestelle für Elektro- und Elektronik-Altgeräte abzugeben.   Die getrennte Sammlung und ordnungsgemäße Entsorgung Ihrer Altgeräte trägt zur Erhaltung der natürlichen Ressourcen bei und garantiert eine Wiederverwertung, die die Gesundheit des Menschen und die Umwelt schützt. Informationen dazu, wo Sie Rücknahmestellen für Ihre Altgeräte finden, erhalten Sie bei Ihrer Stadtverwaltung, den örtlichen Müllentsorgungsbetrieben oder im Geschäft, in dem Sie das Gerät erworben haben

Απόρριψη άχρηστου εξοπλισμού από χρήστες σε ιδιωτικά νοικοκυριά στην Ευρωπαϊκή Ένωση

Το σύμβολο αυτό στο προϊόν ή τη συσκευασία του υποδεικνύει ότι το συγκεκριμένο προϊόν δεν πρέπει να διατίθεται μαζί με τα άλλα οικιακά σας απορρίμματα. Αντίθετα, είναι δική σας ευθύνη να απορρίψετε τον άχρηστο εξοπλισμό σας παραδίδοντάς τον σε καθορισμένο σημείο συλλογής για την ανακύκλωση άχρηστου ηλεκτρικού και ηλεκτρονικού εξοπλισμού. Η ξεχωριστή συλλογή και ανακύκλωση του άχρηστου εξοπλισμού σας κατά την απόρριψη θα συμβάλει στη διατήρηση των φυσικών πόρων και θα διασφαλίσει ότι η ανακύκλωση γίνεται με τρόπο που προστατεύει την ανθρώπινη υγεία και το περιβάλλον. Για περισσότερες πληροφορίες σχετικά με το πού μπορείτε να παραδώσετε τον άχρηστο εξοπλισμό σας για ανακύκλωση, επικοινωνήστε με το αρμόδιο τοπικό γραφείο, την τοπική υπηρεσία διάθεσης οικιακών απορριμμάτων ή το κατάστημα όπου αγοράσατε το προϊόν.

Készülékek magánháztartásban történő selejtezése az Európai Unió területén
A készüléken, illetve a készülék csomagolásán látható azonos szimbólum annak jelzésére szolgál, hogy a készülék a selejtezés során az egyéb háztartási hulladéktól eltérő módon kezelendő. A vásárló a hulladékká vált készüléket köteles a kijelölt gyűjtőhelyre szállítani az elektromos és elektronikai készülékek újrahasznosítása céljából. A hulladékká vált készülékek selejtezéskori begyűjtése és újrahasznosítása hozzájárul a természeti erőforrások megőrzéséhez, valamint biztosítja a selejtezett termékek környezetre és emberi egészségre nézve biztonságos feldolgozását. A begyűjtés pontos helyéről bővebb tájékoztatást a lakhelye szerint illetékes önkormányzattól, az illetékes szemételtakarító vállalattól, illetve a terméket elárusító helyen kaphat.

Smaltimento delle apparecchiature da parte di privati nel territorio dell'Unione Europea
Questo simbolo presente sul prodotto o sulla sua confezione indica che il prodotto non può essere smaltito insieme ai rifiuti domestici. È responsabilità dell'utente smaltire le apparecchiature consegnandole presso un punto di raccolta designato al riciclo e allo smaltimento di apparecchiature elettriche ed elettroniche. La raccolta differenziata e il corretto riciclo delle apparecchiature da smaltire permette di proteggere la salute degli individui e l'ecosistema. Per ulteriori informazioni relative ai punti di raccolta delle apparecchiature, contattare l'ente locale per lo smaltimento dei rifiuti, oppure il negozio presso il quale è stato acquistato il prodotto.

Nolietotu iekārtu iznīcināšanas noteikumi lietotājiem Eiropas Savienības privātajās mājsaimniecībās
Šāds simbols uz izstrādājuma vai uz tā iesaiņojuma norāda, ka šo izstrādājumu nedrīkst izmest kopā ar citiem sadzīves atkritumiem. Jūs atbildat par to, lai nolietotās iekārtas tiktu nodotas speciāli iekārtotos punktos, kas paredzēti izmantoto elektrisko un elektronisko iekārtu savākšanai otrreizējai pārstrādei. Atsevišķa nolietoto iekārtu savākšana un otrreizējā pārstrāde palīdzēs saglabāt dabas resursus un garantēs, ka šīs iekārtas tiks otrreizēji pārstrādātas tādā veidā, lai pasargātu vidi un cilvēku veselību. Lai uzzinātu, kur nolietotās iekārtas var izmest otrreizējai pārstrādei, jāvēršas savas dzīves vietas pašvaldībā, sadzīves atkritumu savākšanas dienestā vai veikalā, kurā izstrādājums tika nopirkts.

Vartotojų iš privačių namų ūkių įrangos atliekų šalinimas Europos Sąjungoje
Šis simbolis ant gaminio arba jo pakuotės rodo, kad šio gaminio šalinti kartu su kitomis namų ūkio atliekomis negalima. Šalintinas įrangos atliekas privalote pristatyti į specialią surinkimo vietą elektros ir elektroninės įrangos atliekoms perdirbti. Atskirai surenkamos ir perdirbamos šalintinos įrangos atliekos padės saugoti gamtinius išteklius ir užtikrinti, kad jos bus perdirbtos tokiu būdu, kuris nekenkia žmonių sveikatai ir aplinkai. Jeigu norite sužinoti daugiau apie tai, kur galima pristatyti perdirbtinas įrangos atliekas, kreipkitės į savo seniūniją, namų ūkio atliekų šalinimo tarnybą arba parduotuvę, kurioje įsigijote gaminį.

Verwijdering van afgedankte apparatuur door privé-gebruikers in de Europese Unie
Dit symbool op het product of de verpakking geeft aan dat dit product niet mag worden gedeponeerd bij het normale huishoudelijke afval. U bent zelf verantwoordelijk voor het inleveren van uw afgedankte apparatuur bij een inzamelingspunt voor het recyclen van oude elektrische en elektronische apparatuur. Door uw oude apparatuur apart aan te bieden en te recyclen, kunnen natuurlijke bronnen worden behouden en kan het materiaal worden hergebruikt op een manier waarmee de volksgezondheid en het milieu worden beschermd. Neem contact op met uw gemeente, het afvalinzamelingsbedrijf of de winkel waar u het product hebt gekocht voor meer informatie over inzamelingspunten waar u oude apparatuur kunt aanbieden voor recycling.

Pozbywanie się zużytego sprzętu przez użytkowników w prywatnych gospodarstwach domowych w Unii Europejskiej

Ten symbol na produkcie lub jego opakowaniu oznacza, że produktu nie wolno wyrzucać do zwykłych pojemników na śmieci. Obowiązkiem użytkownika jest przekazanie zużytego sprzętu do wyznaczonego punktu zbiórki w celu recyklingu odpadów powstałych ze sprzętu elektrycznego i elektronicznego. Osobna zbiórka oraz recykling zużytego sprzętu pomogą w ochronie zasobów naturalnych i zapewnią ponowne wprowadzenie go do obiegu w sposób chroniący zdrowie człowieka i środowisko. Aby uzyskać więcej informacji o tym, gdzie można przekazać zużyty sprzęt do recyklingu, należy się skontaktować z urzędem miasta, zakładem gospodarki odpadami lub sklepem, w którym zakupiono produkt.

Descarte de Lixo Elétrico na Comunidade Européia

Este símbolo encontrado no produto ou na embalagem indica que o produto não deve ser descartado no lixo doméstico comum. É responsabilidade do cliente descartar o material usado (lixo elétrico), encaminhando-o para um ponto de coleta para reciclagem. A coleta e a reciclagem seletivas desse tipo de lixo ajudarão a conservar as reservas naturais; sendo assim, a reciclagem será feita de uma forma segura, protegendo o ambiente e a saúde das pessoas. Para obter mais informações sobre locais que reciclam esse tipo de material, entre em contato com o escritório da HP em sua cidade, com o serviço de coleta de lixo ou com a loja em que o produto foi adquirido.

Likvidácia vyradených zariadení v domácnostiach v Európskej únii

Symbol na výrobku alebo jeho balení označuje, že daný výrobok sa nesmie likvidovať s domovým odpadom. Povinnosťou spotrebiteľa je odovzdať vyradené zariadenie v zbernom mieste, ktoré je určené na recykláciu vyradených elektrických a elektronických zariadení. Separovaný zber a recyklácia vyradených zariadení prispieva k ochrane prírodných zdrojov a zabezpečuje, že recyklácia sa vykonáva spôsobom chrániacim ľudské zdravie a životné prostredie. Informácie o zberných miestach na recykláciu vyradených zariadení vám poskytne miestne zastupiteľstvo, spoločnosť zabezpečujúca odvoz domového odpadu alebo obchod, v ktorom ste si výrobok zakúpili.

Odstranjevanje odslužene opreme uporabnikov v zasebnih gospodinjstvih v Evropski uniji

Ta znak na izdelku ali njegovi embalaži pomeni, da izdelka ne smete odvreči med gospodinjske odpadke. Nasprotno, odsluženo opremo morate predati na zbirališče, pooblaščeno za recikliranje odslužene električne in elektronske opreme. Ločeno zbiranje in recikliranje odslužene opreme prispeva k ohranjanju naravnih virov in zagotavlja recikliranje te opreme na zdravju in okolju neškodljiv način. Za podrobnejše informacije o tem, kam lahko odpeljete odsluženo opremo na recikliranje, se obrnite na pristojni organ, komunalno službo ali trgovino, kjer ste izdelek kupili.

Eliminación de residuos de equipos eléctricos y electrónicos por parte de usuarios particulares en la Unión Europea

Este símbolo en el producto o en su envase indica que no debe eliminarse junto con los desperdicios generales de la casa. Es responsabilidad del usuario eliminar los residuos de este tipo depositándolos en un "punto limpio" para el reciclado de residuos eléctricos y electrónicos. La recogida y el reciclado selectivos de los residuos de aparatos eléctricos en el momento de su eliminación contribuirá a conservar los recursos naturales y a garantizar el reciclado de estos residuos de forma que se proteja el medio ambiente y la salud. Para obtener más información sobre los puntos de recogida de residuos eléctricos y electrónicos para reciclado, póngase en contacto con su ayuntamiento, con el servicio de eliminación de residuos domésticos o con el establecimiento en el que adquirió el producto.

Bortskaffande av avfallsprodukter från användare i privathushåll inom Europeiska Unionen
Om den här symbolen visas på produkten eller förpackningen betyder det att produkten inte får slängas på samma ställe som hushållssopor. I stället är det ditt ansvar att bortskaffa avfallet genom att överlämna det till ett uppsamlingsställe avsett för återvinning av avfall från elektriska och elektroniska produkter. Separat insamling och återvinning av avfallet hjälper till att spara på våra naturresurser och gör att avfallet återvinns på ett sätt som skyddar människors hälsa och miljön. Kontakta ditt lokala kommunkontor, din närmsta återvinningsstation för hushållsavfall eller affären där du köpte produkten för att få mer information om var du kan lämna ditt avfall för återvinning.

Index

— This page is intentionally unused. —

— *This page is intentionally unused.* —