



Designing AirPort Networks Using AirPort Utility

Mac OS X v10.5 + Windows

Contents

Chapter 1	3 Getting Started
	5 Configuring an Apple Wireless Device for Internet Access Using AirPort Utility
	6 Extending the Range of Your AirPort Network
	6 Sharing a USB Hard Disk Connected to an AirPort Extreme Base Station or Time Capsule
	6 Printing with an Apple Wireless Device
	6 Sharing Your Computer's Internet Connection
Chapter 2	9 AirPort Security
	9 Security for AirPort Networks at Home
	10 Security for AirPort Networks in Businesses and Classrooms
	11 Wi-Fi Protected Access (WPA) and WPA2
Chapter 3	14 AirPort Network Designs
	15 Using AirPort Utility
	17 Setting Up the AirPort Extreme Network
	24 Configuring and Sharing Internet Access
	40 Setting Advanced Options
	42 Setting Up a Wireless Distribution System (WDS)
	46 Extending the Range of an 802.11n Network
	48 Setting up a Dual-Band (2.4 GHz and 5 GHz) Network
	49 Keeping Your Network Secure
	54 Directing Network Traffic to a Specific Computer on Your Network (Port Mapping)
	56 Logging
	57 Setting up IPv6
	58 Sharing and Securing USB Hard Disks on Your Network
	60 Using a Time Capsule in Your Network
	60 Connecting a USB Printer to an Apple Wireless Device
	61 Adding a Wireless Client to Your 802.11n Network
	62 Solving Problems
Chapter 4	64 Behind the Scenes
	64 Basic Networking
	67 Items That Can Cause Interference with AirPort
Glossary	69

AirPort offers the easiest way to provide wireless Internet access and networking anywhere in the home, classroom, or office.

AirPort is based on the latest Institute of Electrical and Electronics Engineers (IEEE) 802.11n draft specification and provides fast and reliable wireless networking in the home, classroom, or small office. You can enjoy data transfer rates of up to five times faster than data rates provided by the 802.11g standard and more than twice the network range.

The AirPort Extreme Base Station and Time Capsule are dual-band, so they can work in either the 2.4 gigahertz (GHz) or 5 GHz spectrum. And they are 100 percent backward-compatible, so Mac computers and PCs that use 802.11a, 802.11b, 802.11g, or IEEE draft specification 802.11n wireless cards can connect to an AirPort wireless network. They also work flawlessly with the AirPort Express for wireless music streaming and more. The AirPort Extreme Base Station and Time Capsule have three additional 10/100/1000Base-T Gigabit Ethernet ports, so you don't need to include another router in your network.

To set up an AirPort Extreme Base Station, an AirPort Express, or a Time Capsule, you use AirPort Utility, the easy-to-use setup and management application. AirPort Utility has a simple user experience, with all software controls accessible from the same application. It provides better management of several Apple wireless devices, with client-monitoring features and logging. AirPort Utility enables guest accounts that expire, for temporary access to your network; you no longer need to give your network password to weekend visitors in your home or office. You can even set up accounts with time constraints for the best in parental controls. This version of AirPort Utility supports IPv6 and Bonjour, so you can “advertise” network services such as printing and sharing a hard disk over the WAN port.

Note: When the features discussed in this document apply to the AirPort Extreme Base Station, AirPort Express, and Time Capsule, the devices are referred to collectively as Apple wireless devices.

With an AirPort Extreme Base Station or a Time Capsule, you can connect a USB hard disk so that everyone on the network can back up, store, and share files. Every Time Capsule includes an internal AirPort disk, so you don't need to connect an external one. If you want, you can connect additional USB disks to the USB port on your Time Capsule. You can also connect a USB printer to the USB port on any Apple wireless device, so that everyone on the network can access the printer or hub.

All Apple wireless devices provide strong, wireless security. They offer a built-in firewall and support industry-standard encryption technologies. Yet the simple setup utility and powerful access controls make it easy for authorized users to connect to the AirPort network they create.

You can use an Apple wireless device to provide wireless Internet access and share a single Internet connection among several computers in the following ways:

- Set up the device to act as a router and provide Internet Protocol (IP) addresses to computers on the network using Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT). When the wireless device is connected to a DSL or cable modem that is connected to the Internet, it receives webpages and email content from the Internet through its Internet connection, and then sends the content to wireless-enabled computers, using the wireless network or using Ethernet if there are computers connected to the Ethernet ports.
- Set up the Apple wireless device to act as a bridge on an existing network that already has Internet access and a router providing IP addresses. The device passes IP addresses and the Internet connection to AirPort or wireless-enabled computers, or computers connected to the wireless device by Ethernet.

This document provides information about the AirPort Extreme Base Station, AirPort Express, and Time Capsule, and detailed information about designing 802.11n networks with AirPort Utility for computers using Mac OS X v10.5 or later, and Windows Vista or Windows XP with Service Pack 2. You can set up an Apple wireless device and connect to the Internet without wires in minutes. But because Apple wireless devices are flexible and powerful networking products, you can also create an AirPort network that does much more. If you want to design an AirPort network that provides Internet access to non-AirPort computers via Ethernet, or take advantage of some of your wireless device's more advanced features, use this document to design and implement your network. You can find more general wireless networking information and an overview of AirPort technology in the earlier AirPort documents, located at apple.com/support/manuals/airport.

Note: The images of AirPort Utility in this document are from Mac OS X v10.5. If you are using a Windows computer, the images you see in this document may be slightly different from what you see on your screen.

Configuring an Apple Wireless Device for Internet Access Using AirPort Utility

Like your computer, Apple wireless devices must be set up with the appropriate hardware and IP networking information to connect to the Internet. Install AirPort Utility, which came on the CD with your wireless device, and use it to provide Internet configuration information and other network settings.

This version of AirPort Utility combines the ease of use of AirPort Setup Assistant and the power of AirPort Admin Utility. It is installed in the Utilities folder in the Applications folder on a Macintosh computer using Mac OS X, and in Start > All Programs > AirPort on computers using Windows. AirPort Utility walks you through the setup process by asking a series of questions to determine how the device's Internet connection and other interfaces should be set up. Enter the settings you received from your ISP or network administrator for Ethernet, PPP over Ethernet (PPPoE), or your local area network (LAN); give your AirPort network a name and password; set up a device as a wireless bridge to extend the range of your existing AirPort network; and set other options.

When you have finished entering the settings, AirPort Utility transfers the settings to your wireless device. Then it connects to the Internet and shares its Internet connection with computers that join its AirPort network.

You can also create an AirPort network that takes advantage of the more advanced networking features of Apple wireless devices. To set more advanced AirPort options, use AirPort Utility to manually set up your wireless device's configuration, or make quick adjustments to one you have already set up. Some of the AirPort advanced networking features can be configured only using the manual setup features in AirPort Utility.

Set up your Apple wireless device manually using AirPort Utility when:

- You want to provide Internet access to computers that connect to the wireless device using Ethernet
- You have already set up your device, but you need to change one setting, such as your account credentials
- You need to configure advanced settings such as channel frequency, advanced security options, closed networks, DHCP lease time, access control, WAN privacy, power controls, or port mapping or other options

For instructions on using AirPort Utility to manually set up your wireless device and network, see "Using AirPort Utility" on page 15.

Extending the Range of Your AirPort Network

You can extend the range of your network by using AirPort Utility to set up wireless connections between several devices in your network, known as a Wireless Distribution System (WDS), or to connect a device using Ethernet to create a roaming network. For more information on setting up a WDS or a roaming network, see “Connecting Additional Wireless Devices to Your AirPort Network” on page 40.

Sharing a USB Hard Disk Connected to an AirPort Extreme Base Station or Time Capsule

If you’re using the newest AirPort Extreme Base Station or a Time Capsule, you can connect a USB hard disk to it, and computers connected to the network—wired or wireless, Mac or Windows—can share files using the hard disk. Every Time Capsule includes an internal AirPort disk, so you don’t need to connect an external one. If you want, you can connect additional USB disks to the USB port on your Time Capsule. See “Sharing and Securing USB Hard Disks on Your Network” on page 58.

Printing with an Apple Wireless Device

If you have a compatible USB printer connected to your Apple wireless device, computers on the AirPort network can use Bonjour (Apple’s zero-configuration networking technology) to print to the printer. For instructions about printing to a USB printer from a computer, see “Connecting a USB Printer to an Apple Wireless Device” on page 60.

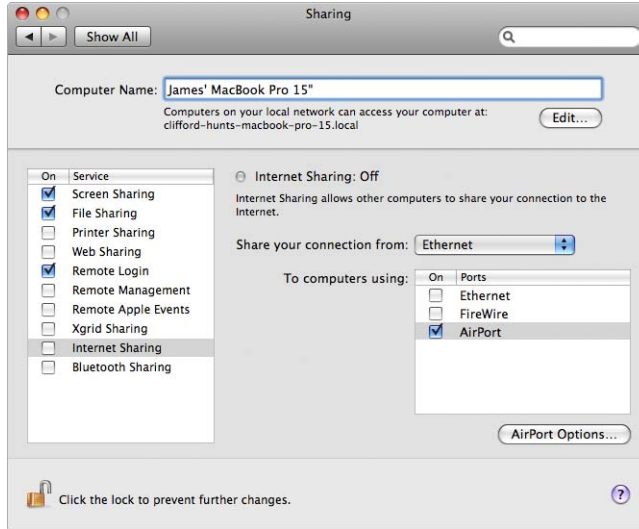
Sharing Your Computer’s Internet Connection

If your computer is connected to the Internet, you can share your Internet connection with other computers using Mac OS X version 10.2 or later, or Windows XP with Service Pack 2. This is sometimes called using your computer as a *software base station*.

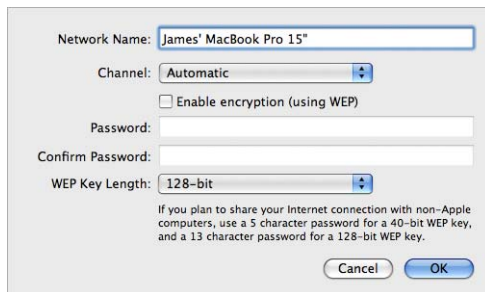
You can share your Internet connection as long as your computer is connected to the Internet. If your computer goes to sleep or is restarted, or if you lose your Internet connection, you need to restart Internet sharing.

To start Internet sharing on a computer using Mac OS X v10.5:

- 1 Open System Preferences and click Sharing.
- 2 Choose the port you want to use to share your Internet connection from the “Share your connection using” pop-up menu.
- 3 Select the port you want to use to share your Internet connection in the “To computers using” list. You can choose to share your Internet connection with AirPort-enabled computers or computers with built-in Ethernet, for example.
- 4 Select Internet Sharing in the Services list.

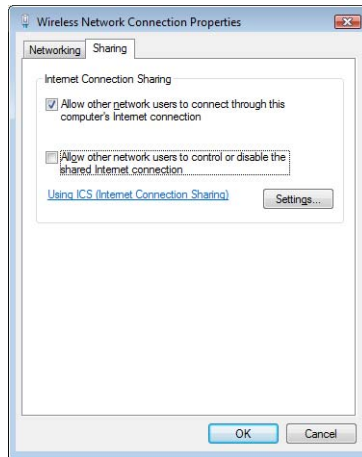


- 5 If you want to share your Internet connection with computers using AirPort, click AirPort Options to give your network a name and password.



To start Internet sharing on a computer using Windows:

- 1 Open Control Panel from the Start menu, and then click “Network and Internet.”
- 2 Click “Network and Sharing Center.”
- 3 Click “Manage network connections” in the Tasks list.
- 4 Right-click the network connection you want to share, and then select Properties.
- 5 Click Sharing and then select “Allow other network users to connect through this computer’s Internet connection.”



Note: If your Internet connection and your local network use the same port (built-in Ethernet, for example), contact your ISP before you turn on Internet sharing. In some cases (if you use a cable modem, for example) you might unintentionally affect the network settings of other ISP customers, and your ISP might terminate your service to prevent you from disrupting its network.

The following chapters explain AirPort security options, AirPort network design and setup, and other advanced options.

This chapter provides an overview of the security features available in AirPort.

Apple has designed its wireless devices to provide several levels of security, so you can enjoy peace of mind when you access the Internet, manage online financial transactions, or send and receive email. The AirPort Extreme Base Station and Time Capsule also include a slot for inserting a lock to deter theft.

For information and instructions for setting up these security features, see “Setting Up the AirPort Extreme Network” on page 17.

Security for AirPort Networks at Home

Apple gives you ways to protect your wireless AirPort network as well as the data that travels over it.

NAT Firewall

You can isolate your wireless network with firewall protection. Apple wireless devices have a built-in Network Address Translation (NAT) firewall that creates a barrier between your network and the Internet, protecting data from Internet-based IP attacks. The firewall is automatically turned on when you set up the device to share a single Internet connection. For computers with a cable or DSL modem, AirPort can actually be safer than a wired connection.

Closed Network

Creating a closed network keeps the network name and the very existence of your network private. Prospective users of your network must know the network name and password to access it. Use AirPort Utility, located in the Utilities folder in the Applications folder on a Macintosh computer using Mac OS X, or in Start > All Programs > AirPort on a computer using Windows, to create a closed network.

Password Protection and Encryption

AirPort uses password protection and encryption to deliver a level of security comparable to that of traditional wired networks. Users can be required to enter a password to log in to the AirPort network. When transmitting data and passwords, the wireless device uses up to 128-bit encryption, through either Wi-Fi Protected Access (WPA), WPA2, or Wired Equivalent Privacy (WEP), to scramble data and help keep it safe. If you are setting up an 802.11n-based AirPort device, you can also use WEP (Transitional Security Network) if both WEP-compatible and WPA/WPA2-compatible computers will join your network.

Note: WPA security is available only to AirPort Extreme wireless devices; AirPort and AirPort Extreme clients using Mac OS X 10.3 or later and AirPort 3.3 or later; and to non-Apple clients using other 802.11 wireless adapters that support WPA. WPA2 security requires firmware version 5.6 or later for an AirPort Extreme Base Station, firmware version 6.2 or later an AirPort Express, firmware version 7.3 or later for a Time Capsule, and a Macintosh computer with an AirPort Extreme wireless card using AirPort 4.2 or later. If your computer uses Windows XP or Windows Vista, check the documentation that came with your computer to see if your computer supports WPA2.

Security for AirPort Networks in Businesses and Classrooms

Businesses and schools need to restrict network communications to authorized users and keep data safe from prying eyes. To meet this need, Apple wireless devices and software provide a robust suite of security mechanisms. Use AirPort Utility to set up these advanced security features.

Transmitter Power Control

Because radio waves travel in all directions, they can extend outside the confines of a specific building. The Transmit Power setting in AirPort Utility lets you adjust the transmission range of your device's network. Only users within the network vicinity have access to the network.

MAC Address Access Control

Every AirPort and wireless card has a unique Media Access Control (MAC) address. For AirPort and AirPort Extreme Cards, the MAC address is sometimes referred to as the AirPort ID. Support for MAC address access control lets administrators set up a list of MAC addresses and restrict access to the network to only those users whose MAC addresses are in the access control list.

RADIUS Support

The Remote Authentication Dial-In User Service (RADIUS) makes securing a large network easy. RADIUS is an access control protocol that allows a system administrator to create a central list of the user names and passwords of computers that can access the network. Placing this list on a centralized server allows many wireless devices to access the list and makes it easy to update. If the MAC address of a user's computer (which is unique to each 802.11 wireless card) is not on your approved MAC address list, the user cannot join your network.

Wi-Fi Protected Access (WPA) and WPA2

There has been increasing concern about the vulnerabilities of WEP. In response, the Wi-Fi Alliance, in conjunction with the IEEE, has developed enhanced, interoperable security standards called Wi-Fi Protected Access (WPA) and WPA2.

WPA and WPA2 use specifications that bring together standards-based, interoperable security mechanisms that significantly increase the level of data protection and access control for wireless LANs. WPA and WPA2 provide wireless LAN users with a high-level assurance that their data remains protected and that only authorized network users can access the network. A wireless network that uses WPA or WPA2 requires all computers that access the wireless network to have WPA or WPA2 support. WPA provides a high level of data protection and (when used in Enterprise mode) requires user authentication.

The main standards-based technologies that constitute WPA include Temporal Key Integrity Protocol (TKIP), 802.1X, Message Integrity Check (MIC), and Extensible Authentication Protocol (EAP).

TKIP provides enhanced data encryption by addressing the WEP encryption vulnerabilities, including the frequency with which keys are used to encrypt the wireless connection. 802.1X and EAP provide the ability to authenticate a user on the wireless network.

802.1X is a port-based network access control method for wired as well as wireless networks. The IEEE adopted 802.1X as a standard in August 2001.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them, and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, the data is assumed to have been tampered with and the packet is dropped. If multiple MIC failures occur, the network may initiate countermeasures.

The EAP protocol known as TLS (Transport Layer Security) presents a user's credentials in the form of digital certificates. A user's digital certificates can comprise user names and passwords, smart cards, secure IDs, or any other identity credentials that the IT administrator is comfortable using. WPA uses a wide variety of standards-based EAP implementations, including EAP-Transport Layer Security (EAP-TLS), EAP-Tunnel Transport Layer Security (EAP-TTLS), and Protected Extensible Authentication Protocol (PEAP). AirPort Extreme also supports the Lightweight Extensible Authentication Protocol (LEAP), a security protocol used by Cisco access points to dynamically assign a different WEP key to each user. AirPort Extreme is compatible with Cisco's LEAP security protocol, enabling AirPort users to join Cisco-hosted wireless networks using LEAP.

In addition to TKIP, WPA2 supports the AES-CCMP encryption protocol. Based on the very secure AES national standard cipher, combined with sophisticated cryptographic techniques, AES-CCMP was specifically designed for wireless networks. Migrating from WEP to WPA2 requires new firmware for the AirPort Extreme Base Station (version 5.6 or later), and for AirPort Express (version 6.2 or later). Devices using WPA2 mode are not backward compatible with WEP.

WPA and WPA2 have two modes:

- Personal mode, which relies on the capabilities of TKIP or AES-CCMP without requiring an authentication server
- Enterprise mode, which uses a separate server, such as a RADIUS server, for user authentication

WPA and WPA2 Personal

- For home or Small Office/Home Office (SOHO) networks, WPA and WPA2 runs in Personal mode, taking into account that the typical household or small office does not have an authentication server. Instead of authenticating with a RADIUS server, users manually enter a password to log in to the wireless network. When a user enters the password correctly, the wireless device starts the encryption process using TKIP or AES-CCMP. TKIP or AES-CCMP take the original password and derive encryption keys mathematically from the network password. The encryption key is regularly changed and rotated so that the same encryption key is never used twice. Other than entering the network password, the user isn't required to do anything to make WPA or WPA2 Personal work in the home.

WPA and WPA2 Enterprise

WPA is a subset of the draft IEEE 802.11i standard and effectively addresses the wireless local area network (WLAN) security requirements for the enterprise. WPA2 is a full implementation of the ratified IEEE 802.11i standard. In an enterprise with IT resources, WPA should be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. With this implementation in place, the need for add-on solutions such as virtual private networks (VPNs) may be eliminated, at least for securing wireless connections in a network.

For more information about setting up a WPA or WPA2 protected network, see “Using Wi-Fi Protected Access” on page 50.

This chapter provides overview information and instructions for the types of AirPort Extreme networks you can set up, and some of the advanced options of AirPort Extreme.

Use this chapter to design and set up your AirPort Extreme network.

Configuring your Apple wireless device to implement a network design requires three steps:

Step 1: Setting Up the AirPort Extreme Network

Computers communicate with the wireless device over the AirPort wireless network. When you set up the AirPort network created by the wireless device, you can name the wireless network, assign a password that will be needed to join the wireless network, and set other options.

Step 2: Configuring and Sharing Internet Access

When computers access the Internet through the AirPort Extreme network, the wireless device connects to the Internet and transmits information to the computers over the AirPort Extreme network. You provide the wireless device with settings appropriate for your ISP and configure how the device shares this connection with other computers.

Step 3: Setting Advanced Options

These settings are optional for most users. They include using the Apple wireless device as a bridge between your AirPort Extreme network and an Ethernet network, setting advanced security options, setting up a Wireless Distribution System (WDS) to extend the AirPort network to other wireless devices, and fine-tuning other settings.

For specific instructions on all these steps, refer to the sections later in this chapter.

You can do most of your setup and configuration tasks using AirPort Utility, and following the onscreen instructions to enter your ISP and network information. To set advanced options, you need to use AirPort Utility to manually set up your Apple wireless device and AirPort network.

Using AirPort Utility

To set up and configure your computer or Apple wireless device to use AirPort Extreme for basic wireless networking and Internet access, use AirPort Utility and answer a series of questions about your Internet settings and how you would like to set up your network.

- 1 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer.



- 2 Select your device in the list on the left if there is more than one device in your network. Click Continue, and then follow the onscreen instructions to enter the settings from your ISP or network administrator for the type of network you want to set up. See the network diagrams later in this chapter for the types of networks you can set up using AirPort Utility.

To set up a more complicated network, or to make adjustments to a network you have already set up, use the manual setup features in AirPort Utility.

Setting AirPort preferences

Use AirPort preferences to set up your wireless device to alert you when there are updates available for your device. You can also set it up to notify you if there are problems detected, and to provide instructions to help solve the problems.

To set AirPort preferences:

- 1 Open AirPort Utility, located in the Utilities folder inside the Applications folder on a Mac, and in Start > All Programs > AirPort on a Windows computer.
- 2 Choose Preferences from the AirPort Utility menu on a Mac, and from the File menu on a Windows computer.

Select from the following checkboxes:

- Select “Check for Updates when opening AirPort Utility” to automatically check the Apple website for software and firmware updates each time you open AirPort Utility.
- Select the “Check for updates” checkbox, and then choose a time interval from the pop-up menu, such as weekly, to check for software and firmware updates in the background. AirPort Utility opens if updates are available.
- Select “Monitor Apple wireless devices for problems” to investigate problems that may cause the device's status light to blink amber. With the checkbox selected, AirPort Utility opens if a problem is detected, and then provides instructions to help resolve the problem. This option monitors all of the wireless devices on the network.
- Select “Only Apple wireless devices that I have configured” to monitor only the devices you have set up using this computer.

Monitoring devices for problems requires an AirPort wireless device that supports firmware version 7.0 or later.

To set up your wireless device manually:

- 1 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer.
- 2 Select your device in the list.
- 3 Choose Manual Setup from the Base Station menu and enter the password if necessary. The default device password is *public*.

If you don't see your wireless device in the list:

- 1 Open the AirPort status menu in the menu bar on a Mac and make sure that you have joined the AirPort network created by your wireless device. On a Windows computer, hover the cursor over the wireless network icon in the status tray to make sure the computer is connected to the correct network.

The default network name for an Apple wireless device is AirPort Network XXXXXX, where XXXXXX is replaced with the last six digits of the AirPort ID, (or MAC address). The AirPort ID is printed on the bottom of Apple wireless devices.

- 2 Make sure your computer's network and TCP/IP settings are configured properly.
On a computer using Mac OS X, choose AirPort from the Show pop-up menu in the Network pane of System Preferences. Then choose Using DHCP from the Configure IPv4 pop-up menu in the TCP/IP pane.

On a computer using Windows, right-click the wireless connection icon that displays the AirPort network, and choose Status. Click Properties, select Internet Protocol (TCP/IP), and then click Properties. Make sure “Obtain an IP address automatically” is selected.

If you can't open the wireless device settings:

- 1 Make sure your network and TCP/IP settings are configured properly.

On a computer using Mac OS X, select AirPort from the network connection services list in the Network pane of System Preferences. Click Advanced, and then choose Using DHCP from the Configure IPv4 pop-up menu in the TCP/IP pane.

On a computer using Windows, right-click the wireless connection icon that displays the AirPort network, and choose Status. Click Properties, select Internet Protocol (TCP/IP), and then click Properties. Make sure “Obtain an IP address automatically” is selected.

- 2 Make sure you entered the wireless device password correctly. The default password is *public*. If you have forgotten the device password, you can reset it to *public* by resetting the device.

To temporarily reset the device password to *public*, press and hold the reset button for one second. To reset the device back to its default settings, hold the reset button for five full seconds.

If you are on an Ethernet network that has other devices, or you are using Ethernet to connect to the device:

AirPort Utility scans the Ethernet network to create the list of devices. As a result, when you open AirPort Utility, you may see devices that you cannot configure.

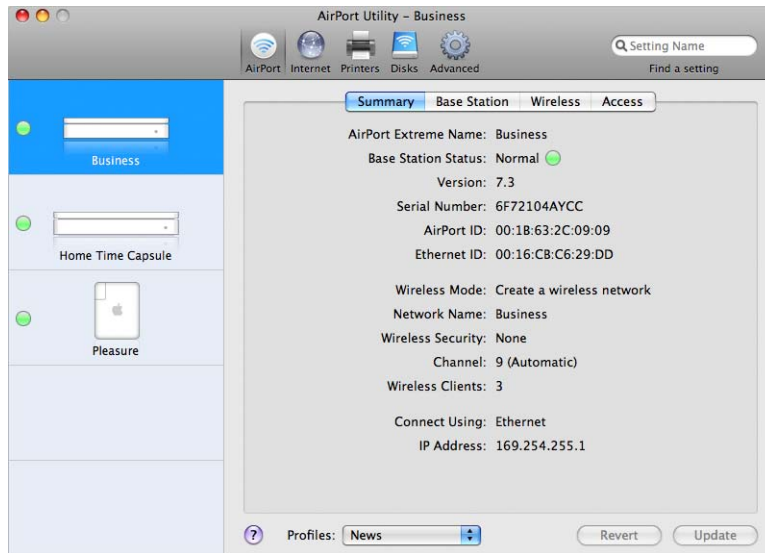
Setting Up the AirPort Extreme Network

The first step in configuring your Apple wireless device is setting up the device and the network it will create. You can set up most features using AirPort Utility and following the onscreen instructions to enter the information from your ISP or network administrator.

To configure a network manually or set advanced options, open your wireless device’s configuration in AirPort Utility and manually set up your device and network.

- 1 Choose the network of the wireless device you want to configure from the AirPort status menu on a computer using Mac OS X, or from the wireless connection icon in the status tray on a computer using Windows.
- 2 Open AirPort Utility and select the wireless device from the list. If you don’t see the device you want to configure, click Rescan to scan for available wireless devices, and then select the one you want from the list.

- 3 Choose Manual Setup from the Base Station menu and enter the password if necessary. The default device password is *public*.



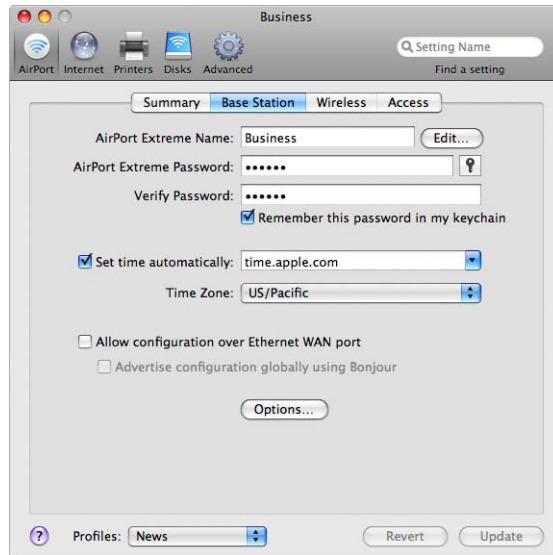
You can also double-click the name of the wireless device to open its configuration in a separate window. When you open the manual setup window, the Summary pane is displayed. The summary pane provides information and status about your wireless device and network.



If the wireless device reports a problem, the status icon turns yellow. Click Base Station Status to display the problem and suggestions to resolve it.

Wireless Device Settings

Click the AirPort button, and then click Base Station. Use the Base Station pane of AirPort Utility to enter information about the wireless device.



Give the Wireless Device a Name

Give the device an easily identifiable name. This makes it easy for administrators to locate a specific device on an Ethernet network with several devices.

Change the Wireless Device Password

The device password protects its configuration so that only the administrator can modify it. The default password is *public*. It is a good idea to change the device password to prevent unauthorized changes to it.

If the password is not changed from *public*, you will not be prompted for a password when you select it from the list and click Configure.

Other Information

- Allow configuration over the WAN port. This allows you to administer the wireless device remotely.
- Advertise the wireless device over the Internet using Bonjour. If you have an account with a dynamic DNS service, you can connect to it over the Internet.
- Set the device time automatically. If you have access to a Network Time Protocol server, whether on your network or on the Internet, choose it from the pop-up menu. This ensures your wireless device is set to the correct time.

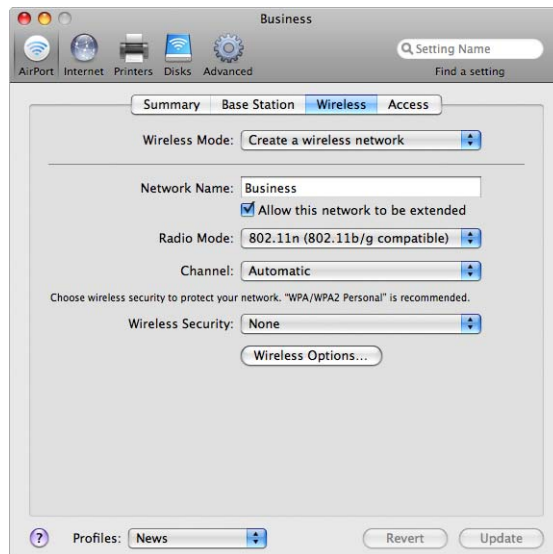
Set Base Station Options

Click Base Station Options and set the following:

- Enter a contact name and location for the wireless device. The name and location are included in some logs the device generates. The contact and location fields may be helpful if you have more than one wireless device on your network.
- Set status light behavior to either Always On or Flash On Activity. If you choose Flash On Activity, the device status light blinks when there is network traffic.
- If your wireless device supports it, select “Check for firmware updates” and choose an increment, such as Daily from the pop-up menu.

Wireless Network Settings

Click Wireless, and enter the network name, radio mode, and other wireless information.



Setting the Wireless Mode

AirPort Extreme supports three wireless modes:

- **Create a wireless network.** Choose this option if you are creating a new AirPort Extreme network.
- **Participate in a WDS network.** Choose this option if you are creating a new WDS network, or connecting this Apple wireless device to a WDS network that is already set up.
- **Extend a wireless network.** Choose this option if you plan to connect another Apple wireless device to the network you are setting up.

Naming the AirPort Extreme Network

Give your AirPort network a name. This name appears in the AirPort status menu on the AirPort-enabled computers that are in range of your AirPort network.

Choosing the Radio Mode

Choose “802.11n (802.11b/g compatible)” from the Radio Mode pop-up menu if computers with 802.11n, 802.11g, or 802.11b wireless cards will join the network. Each client computer will connect to the network and transmit network traffic at the highest possible speed.

Choose “802.11n only (2.4 GHz)” if only computers with 802.11n compatible wireless cards will join the network in the 2.4 GHz frequency range.

Choose “802.11n (802.11a compatible)” if computers with 802.11n and 802.11a wireless cards will join the network in the 5 GHz frequency range. Computers with 802.11g or 802.11b wireless cards will not be able to join this network.

Choose “802.11n only (5 GHz)” if computers with 802.11n wireless cards will join the network. The transmission rate of the network will be at 802.11n speed. Computers with 802.11g, 802.11b, and 802.11a wireless cards will not be able to join this network.

Note: If you don’t want to use an 802.11n radio mode, hold down the Option key and chose a radio mode that doesn’t include 802.11n.

Changing the Channel

The “channel” is the radio frequency over which your wireless device communicates. If you use only one device (for example, at home), you probably won’t need to change the channel frequency. If you set up several wireless devices in a school or office, use different channel frequencies for devices that are within approximately 150 feet of each other.

Adjacent wireless devices should have at least 4 channels between their channel frequencies. So if device A is set to channel 1, device B should be set to channel 6 or 11. For best results, use channels 1, 6, or 11 when operating your device in the 2.4 GHz range.

AirPort-enabled computers automatically tune to the channel frequency your wireless device is using when they join the AirPort network. If you change the channel frequency, AirPort client computers do not need to make any changes.

Note: If you set your wireless device’s radio mode to “802.11n only (5 GHz),” you cannot change the channel. The 5 GHz frequency mode automatically chooses the channel.

Password-protect Your Network

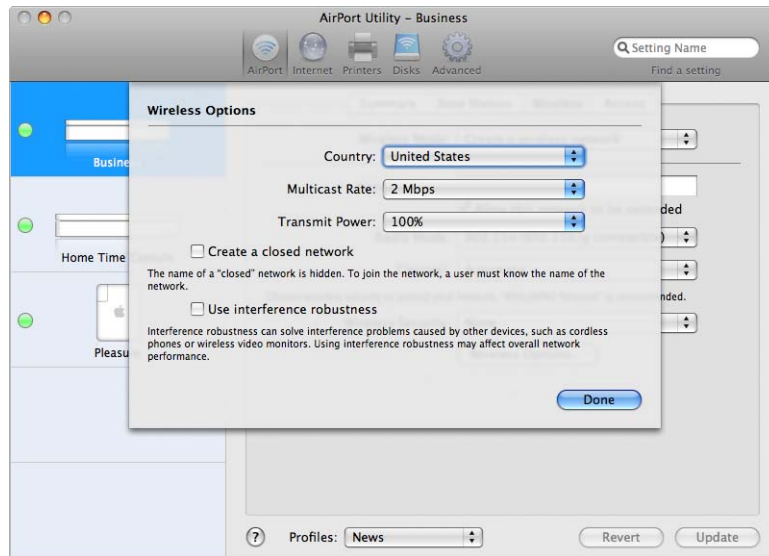
To password-protect your network, you can choose from a number of wireless security options. In the AirPort pane of AirPort Utility, click Wireless and choose one of the following options from the Wireless Security pop-up menu:

- **None:** Choosing this option turns off all password protection for the network. Any computer with a wireless adapter or card can join the network, unless the network is set up to use access control. See “Setting Up Access Control” on page 51.
- **WEP:** If your device supports it, choose this option and enter a password to protect your network with a Wired Equivalent Privacy (WEP) password. Your Apple wireless device supports 40-bit and 128-bit encryption. To use 40-bit WEP, don’t use an 802.11n radio mode.
- **WEP (Transitional Security Network):** If your device supports it, you can use this option to allow computers using WPA or WPA2 to join the network. Computers or devices that use WEP can also join the network. WEP (Transitional Security Network) supports 128-bit encryption. To use this option, the wireless device use an 802.11n radio mode.
- **WPA/WPA2 Personal:** Choose this option to protect your network with Wi-Fi Protected Access. You can use a password between 8 and 63 ASCII characters or a Pre-Shared Key of exactly 64 hexadecimal characters. Computers that support WPA and computers that support WPA2 can join the network. Choose WPA2 Personal if you want only computers that support WPA2 to join your network.
- **WPA/WPA2 Enterprise:** Choose this option if you are setting up a network that includes an authentication server, such as a RADIUS server, with individual user accounts. Enter the IP address and port number for the primary and optional secondary server, and enter a “shared secret,” which is the password for the server. Choose WPA2 Enterprise if you want only computers that support WPA2 to join the network.

For more information and instructions for setting up WPA or WPA2 on your network, see “Using Wi-Fi Protected Access” on page 50.

Setting Wireless Options

Click Wireless Options to set additional options for your network.



Setting Additional Wireless Options

Use the Wireless Options pane to set the following:

- **Region:** Set the region code for the location of your network.
- **Multicast rate:** Choose a multicast rate from the pop-up menu. If you set the multicast rate high, only clients on the network that are within range and can achieve the speed you set will receive transmissions.
- **Transmit power:** Choose a setting from the Transmit Power pop-up menu to set the network range (the lower the percentage, the shorter the network range).
- **WPA Group Key Timeout:** Enter a number in the text field, and choose an increment from the pop-up menu to change the frequency of key rotation.
- **Use Wide Channels:** If you set up your network to use the 5 GHz frequency range, you can use wide channels to provide higher network throughput.

Note: Using wide channels is not permitted in some countries.

- **Create a closed network:** Selecting a closed network hides the name of the network so that users must enter the exact network name and password to join the AirPort Extreme network.
- **Use interference robustness:** Interference robustness can solve interference problems caused by other devices or networks.

To set more advanced security options, see “Keeping Your Network Secure” on page 49.

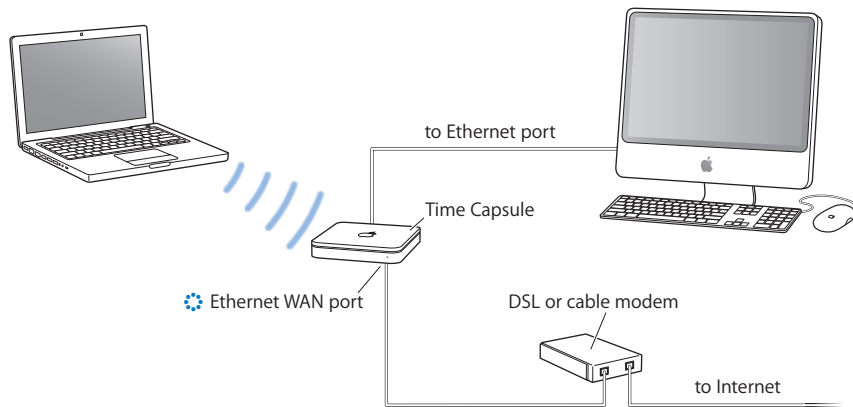
Configuring and Sharing Internet Access

The next step is setting up your wireless device's Internet connection and sharing its Internet access with client computers. The following sections tell you what to do, depending on how your device connects to the Internet.

You're Using a DSL or Cable Modem

In most cases, you can implement this network design using AirPort Utility and following the onscreen instructions to set up your wireless device and network. You need to use AirPort Utility to manually set up your device only if you want to set up or adjust optional advanced settings.

What It Looks Like



How It Works

- The Apple wireless device (in this example, a Time Capsule) connects to the Internet through its Internet WAN (🌐) connection to your DSL or cable modem.
- Computers using AirPort or computers connected to the wireless device's Ethernet LAN port (↔) connect to the Internet through the device.
- The device is set up to use a single, public IP address to connect to the Internet, and uses DHCP and NAT to share the Internet connection with computers on the network using private IP addresses.
- AirPort computers and Ethernet computers communicate with one another through the wireless device.

Important: Connect Ethernet computers that are not connected to the Internet to the device's LAN port (↔) only. Since the device can provide network services, you must set it up carefully to avoid interfering with other services on your Ethernet network.

What You Need for a DSL or Cable Modem Connection

Components	Check	Comments
Internet account with DSL or cable modem service provider	Does your service provider use a static IP or DHCP configuration?	You can get this information from your service provider or the Network preferences pane on the computer you use to access the Internet through this service provider.
Apple wireless device (an AirPort Extreme Base Station, an AirPort Express, or a Time Capsule)		Place the device near your DSL or cable modem.

What to Do

If you are using AirPort Utility to assist you with configuring the Apple wireless device for Internet access:

- 1 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer.
- 2 Follow the onscreen instructions and enter the settings you received from your service provider to connect to the Internet, and then set up the device to share the Internet connection with computers on the network.

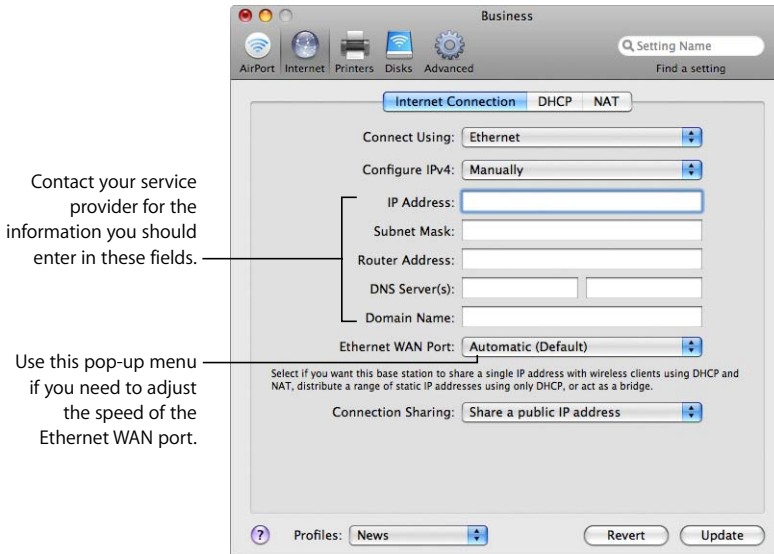
If you are using AirPort Utility to manually set up your wireless device:

- 1 Make sure that your DSL or cable modem is connected to the Ethernet WAN port (🌐) on your Apple wireless device.
- 2 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer. Select your wireless device and choose Manual Setup from the Base Station menu, or double-click your device's icon in the list to open the configuration in a separate window.
- 3 Click the Internet button. Click Internet Connection and choose Ethernet or PPPoE from the Connect Using pop-up menu, depending on which one your service provider requires. If your service provider gave you PPPoE connection software, such as EnterNet or MacPoET, choose PPPoE.

Note: If you are connecting to the Internet through a router using PPPoE and your Apple wireless device is connected to the router via Ethernet, you do not need to use PPPoE on your wireless device. Choose Ethernet from the Connect Using pop-up menu in the Internet pane, and deselect the “Distribute IP addresses” checkbox in the Network pane. Contact your service provider if you aren't sure which one to select.

- 4 Choose Manually or Using DHCP from the Configure IPv4 pop-up menu if you chose Ethernet from the Connect Using pop-up menu, depending on how your service provider provides IP addresses.

- If your provider gave you an IP address and other numbers with your subscription, use that information to configure the wireless device IP address manually. If you aren't sure, ask your service provider. Enter the IP address information in the fields below the Configure IPv4 pop-up menu.
- If you chose PPPoE, your ISP provides your IP address automatically using DHCP.



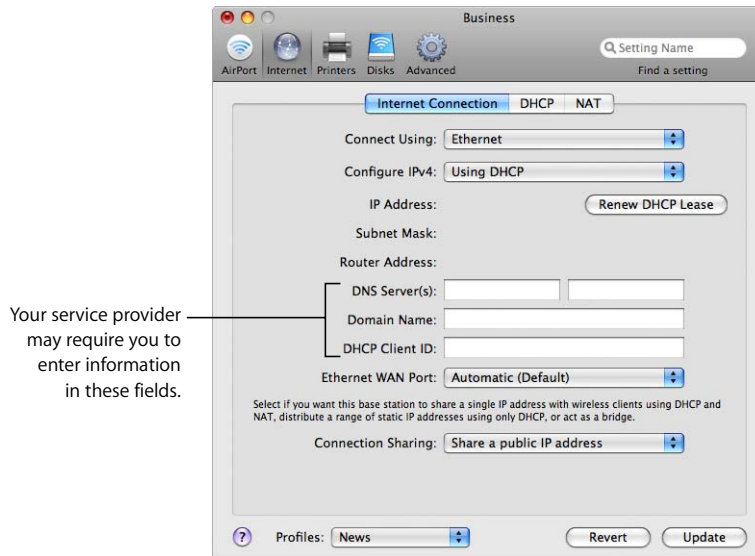
If your service provider asks you for the MAC address of your wireless device, use the address of the Ethernet WAN port (⚙️), printed on the label on the bottom of the device.

If you have already used AirPort Utility to set up your wireless device, the fields below the Configure IPv4 pop-up menu may already contain the information appropriate for your service provider.

You can change the WAN Ethernet speed if you have specific requirements for the network you are connected to. In most cases, the settings that are configured automatically are correct. Your service provider should be able to tell you if you need to adjust these settings.

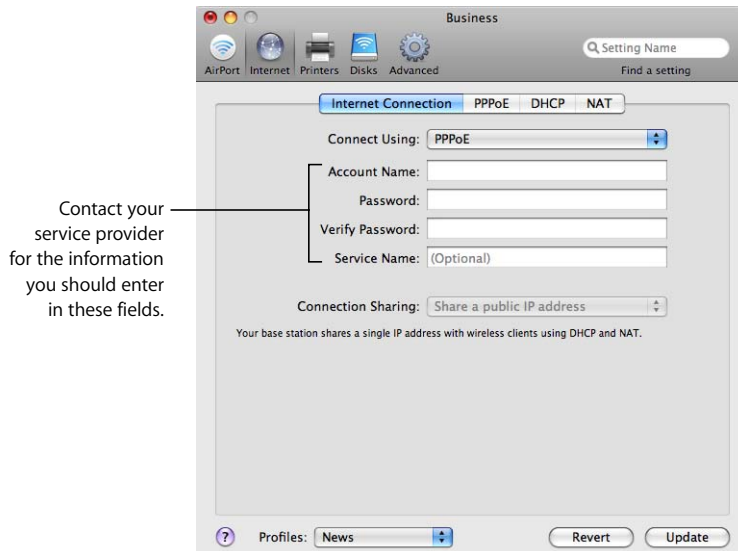
Changing the WAN Ethernet speed can affect the way the wireless device interacts with the Internet. Unless your service provider has given you specific settings, use the automatic settings. Entering the wrong settings can affect network performance.

If you configure TCP/IP using DHCP, choose Using DHCP from the Configure IPv4 pop-up menu. Your IP information is provided automatically by your ISP using DHCP.



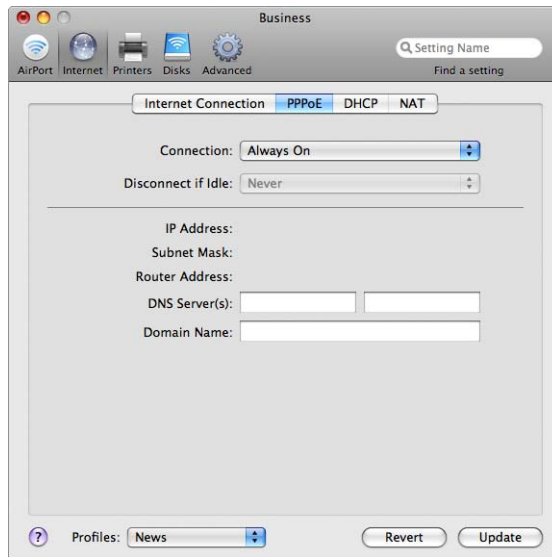
- 5 If you chose PPPoE from the Connect Using pop-up menu, enter the PPPoE settings your service provider gave you. Leave the Service Name field blank unless your service provider requires a service name.

Note: With AirPort, you don't need to use a third-party PPPoE connection application. You can connect to the Internet using AirPort.



If you are connecting to the Internet through a router that uses PPPoE to connect to the Internet, and your wireless device is connected to the router via Ethernet, you do not need to use PPPoE on your device. Choose Ethernet from the Connect Using pop-up menu in the Internet pane, and deselect the “Distribute IP addresses” checkbox in the Network pane. Because your router is distributing IP addresses, your wireless device doesn’t need to. More than one device on a network providing IP addresses can cause problems.

- 6 Click PPPoE to set PPPoE options for your connection.



- Choose Always On, Automatic, or Manual, depending on how you want to control when your wireless device is connected to the Internet.

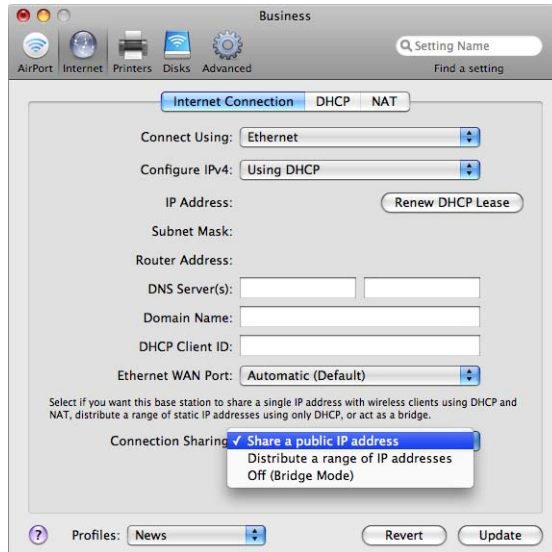
If you choose Always On, your device stays connected to your modem and the Internet as long as the modem is turned on. If you choose Automatic, the wireless device connects to the modem, which connects to the Internet when you use an application that requires an Internet connection, such as email or an instant message or web application. If you choose Manual, you need to connect the modem to the Internet when you use an application that requires an Internet connection.

If you chose Automatic or Manual from the Connection pop-up menu, you need to choose an increment, such as “10 minutes,” from the “Disconnect if idle” pop-up menu. If you don’t require an Internet application after the increment of time has passed, you will be disconnected from the Internet.

Note: If your wireless device is connected to your modem using an Ethernet LAN port, and your modem is connected to the Internet using PPPoE, you may not be able to use the manual setting.

- Enter Domain Name System (DNS) server addresses and a specific domain name your wireless device accesses when you connect to the Internet.
- 7 Click the Network button and configure how the device will share its Internet access with AirPort and Ethernet computers.

If you chose Ethernet from the Connect Using pop-up menu, choose how your device will share the Internet connection from the Connection Sharing pop-up menu.



- To share a single Internet connection with AirPort computers and computers connected to the device with Ethernet using DHCP and NAT, choose “Share a public IP address” from the Connection Sharing pop-up menu. Using DHCP and NAT lets the wireless device dynamically and automatically assign IP addresses to client computers, which simplifies each computer’s TCP/IP configuration. See “Setting DHCP and NAT Options” on page 30.

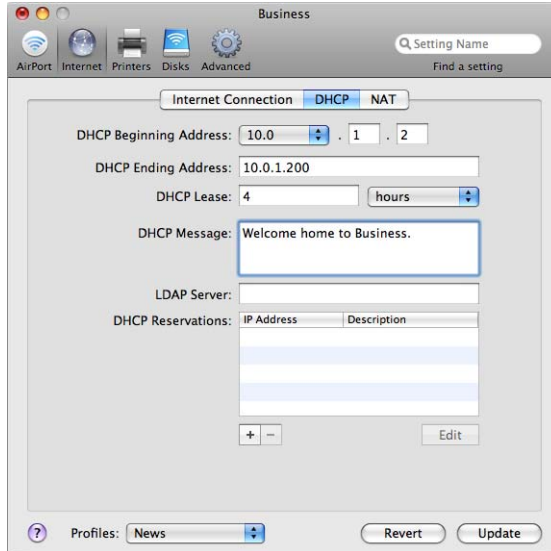
By default, the wireless device allows other devices, computers using Ethernet, and computers using AirPort to communicate with each other using non-IP protocols like AppleTalk. If you want to connect an AppleTalk Ethernet printer to the Apple wireless device or use AppleTalk between wired and wireless computers, make sure the devices are connected to the Ethernet LAN port (↔) on the device.

- To distribute a range of IP addresses using only DHCP, choose “Distribute a range of IP addresses.” See “Setting DHCP Only Options” on page 32.
- If you don’t want your wireless device to share its IP address, choose “Off (Bridge Mode).” If you set up your device in bridge mode, AirPort computers have access to all services on the Ethernet network, and the device does not provide Internet sharing services. See “You’re Using an Existing Ethernet Network” on page 36 for more information about setting up your wireless device as a bridge.

Using the wireless device as a bridge can be a way to address incompatibilities between the device's Internet sharing features and your ISP's connection method.

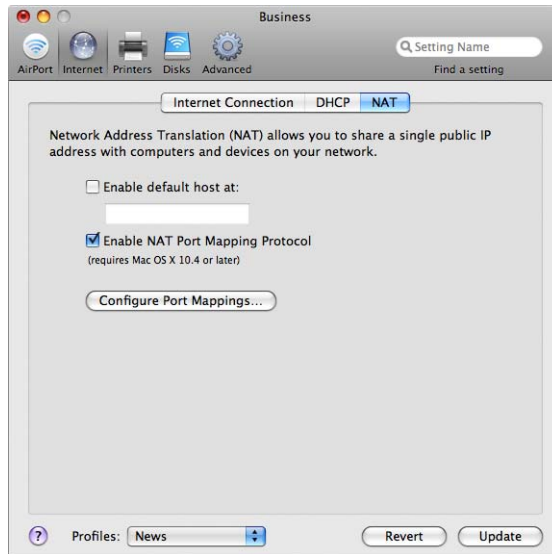
Setting DHCP and NAT Options

If you chose "Share a public IP address" from the Connection Sharing pop-up menu, you can set DHCP and NAT options. Click DHCP.



- Choose a range of IP addresses from the DHCP Range pop-up menu. Choose 10.0, 192.168, or 172.16 and then enter a beginning and ending address in the DHCP Beginning Address and the DHCP Ending Address fields, depending on which addresses you want the wireless device to provide.
- Enter a number in the DHCP Lease field, and then choose minutes, hours, or days from the pop-up menu.
- Type a welcome message in the DHCP Message field. This message is displayed when a computer joins your network.
- If your network is set up to use a Lightweight Directory Access Protocol (LDAP) server on your network, you can enter the address of the server in the LDAP Server field, and computers on your network will have access to it.
- To provide specific IP addresses to specific computers on your wireless network, click the Add (+) button below the DHCP Reservations list, and follow the onscreen instructions to name the reservation and reserve the address by MAC address or DHCP client ID. If you choose MAC address, click Continue and enter the MAC address and specific IP address.

Next you can set NAT options for the network. Click NAT.



- You can set up a default on your network. A default host (sometimes known as a DMZ) is a computer on your network that is exposed to the Internet and receives all inbound traffic. A default host may be useful if you use a computer on your AirPort network to play network games, or want to route all Internet traffic through a single computer.
- You can set up NAT Port Mapping Protocol (NAT-PMP). NAT-PMP is an Internet Engineering Task Force Internet Draft, an alternative to the more common Universal Plug and Play (UPnP) protocol implemented in many network address translation (NAT) routers. NAT-PMP allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact this computer.

Included in the protocol is a method for retrieving the public IP address of a NAT gateway, allowing a client to make this public IP address and port number known to peers that may wish to communicate with it. This protocol is implemented in current Apple products, including Mac OS X 10.4 Tiger, AirPort Extreme and AirPort Express networking products, and Bonjour for Windows.

You can also set up port mapping. To ensure that requests are properly routed to your web, AppleShare, or FTP server, or a specific computer on your network, you need to establish a permanent IP address for the server or computer, and provide “inbound port mapping” information to the Apple wireless device. See “Directing Network Traffic to a Specific Computer on Your Network (Port Mapping)” on page 54.

Setting DHCP Only Options

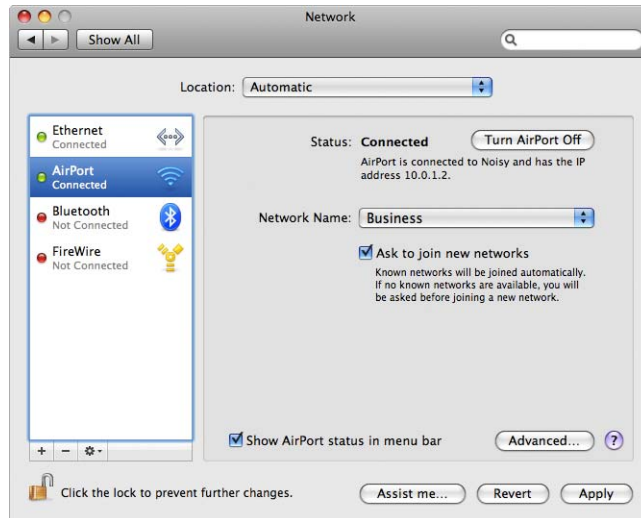
If you chose “Distribute a range of IP addresses” from the Connection Sharing pop-up menu, your wireless device is set up to use DHCP to distribute a range of IP addresses using only DHCP. You cannot use NAT if you chose this option. Click DHCP and enter the beginning and ending addresses you want to distribute to computers joining your wireless network.

You can set the additional DHCP options, such as DHCP Lease, DHCP Message, and other options following the instructions above.

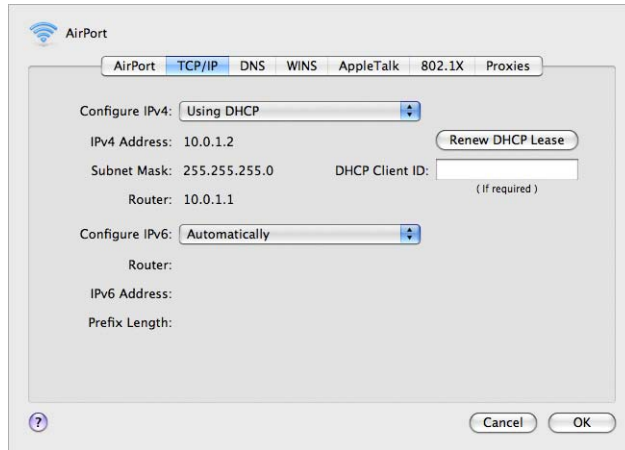
Setting Up Client Computers

To configure TCP/IP on client computers using Mac OS X v10.5:

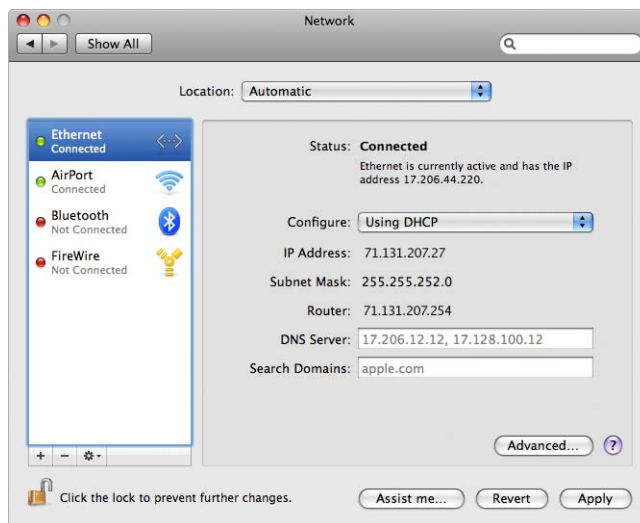
- 1 Open System Preferences on the client computer and then click Network.
- 2 Do one of the following:
 - a If the client computer is using AirPort, select AirPort in the network connection services list, and then click Advanced.



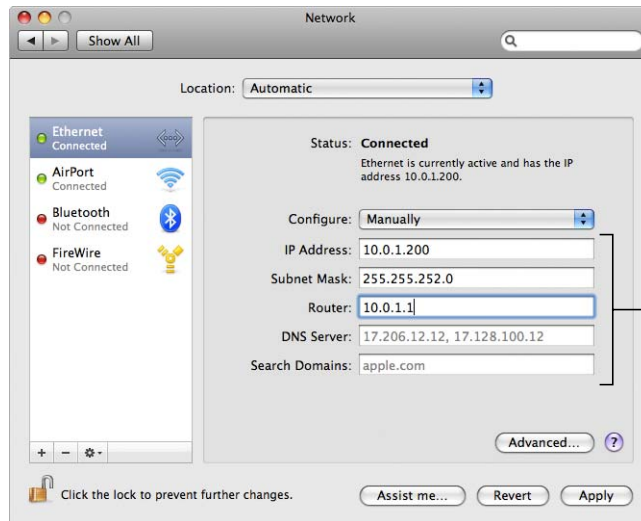
Next, choose DHCP from the Configure IPv4 pop-up menu.



- b If you enabled a DHCP server when you set up the wireless device's network, and the client computer is using Ethernet, select Ethernet in the network connection services list, and then choose Using DHCP from the Configure pop-up menu.



- c If you selected “Distribute a range of IP addresses” when you set up the wireless device’s network, you can provide Internet access to client computers using Ethernet by setting the client IP addresses manually. Select Ethernet in the network connection services list, and then choose Manually from the Configure pop-up menu.



Enter the IP and router addresses from the range your device is providing. Enter the DNS and Search Domain addresses if necessary.

When you configure Ethernet clients manually for a wireless device that provides NAT over Ethernet, you can use IP addresses in the range 10.0.1.2 to 10.0.1.200.

In the Subnet Mask field, enter 255.255.255.0. In the Router field, enter 10.0.1.1.

Enter the same name server address and search domain information that you entered in the wireless device configuration.

To configure TCP/IP on client computers using Windows

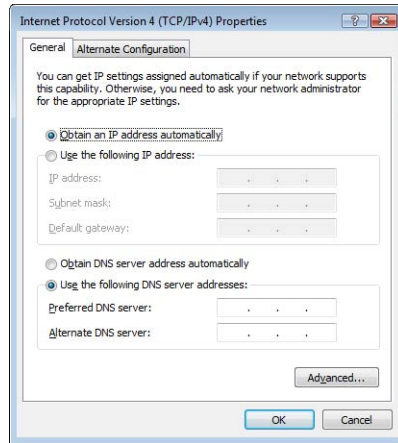
Make sure you have installed the wireless adapter in your computer and the software necessary to set up the adapter.

To configure TCP/IP on client computers:

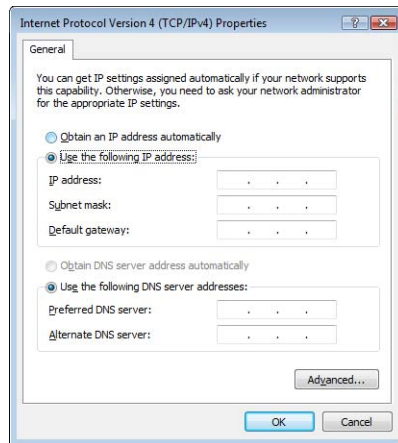
- 1 Open Control Panel from the Start menu, and then click “Network and Internet.”
- 2 Click “Network and Sharing Center.”
- 3 Click “Manage network connections” in the Tasks list.
- 4 Right-click the wireless connection you want to share, and then select Properties.

5 Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties.

- If you chose “Share a public IP address” in the Network pane of AirPort Utility, select “Obtain an IP address automatically.”



- If you chose “Distribute a range of IP addresses” when you set up the wireless device’s network, you can provide Internet access to client computers by setting the client IP addresses manually. Select “Use the following IP address.”



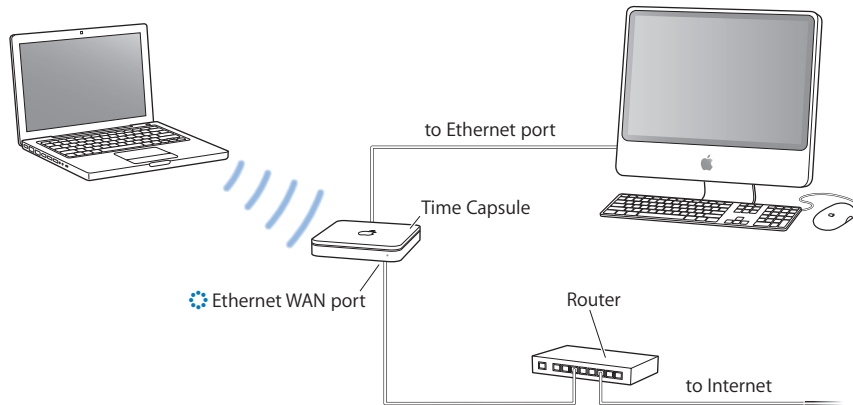
When you configure clients manually for a wireless device that provides NAT service, use IP addresses in the range 10.0.1.2 to 10.0.1.200, 172.16.1.2 to 172.16.1.200, or 192.168.1.2 to 192.168.1.200.

In the “Subnet mask” field, enter 255.255.255.0. In the “Default gateway” field, enter 10.0.1.1, 172.16.1.1, or 192.168.1.1, depending on which addressing scheme you used. Enter the same name server address and search domain information that you entered in the wireless device configuration.

You're Using an Existing Ethernet Network

You can use AirPort Utility to easily set up the Apple wireless device for Internet access through an existing Ethernet network that already has a router, switch, or other network device providing IP addresses. Use the manual setup features of AirPort Utility if you need to adjust optional advanced settings.

What It Looks Like



How It Works

- The Apple wireless device (in this example, a Time Capsule) uses your Ethernet network to communicate with the Internet through the Ethernet LAN port (↔).
- AirPort and Ethernet clients access the Internet and the Ethernet network through the Apple wireless device.

What You Need for an Ethernet Connection

Components	Comments
Apple wireless device (an AirPort Extreme Base Station, an AirPort Express, or a Time Capsule)	Set the device up in bridge mode.
Ethernet router, switch, or other network device	The router, switch, or other network device is set up to provide IP addresses to computers and devices on the Ethernet network.
Ethernet cables	

What to Do

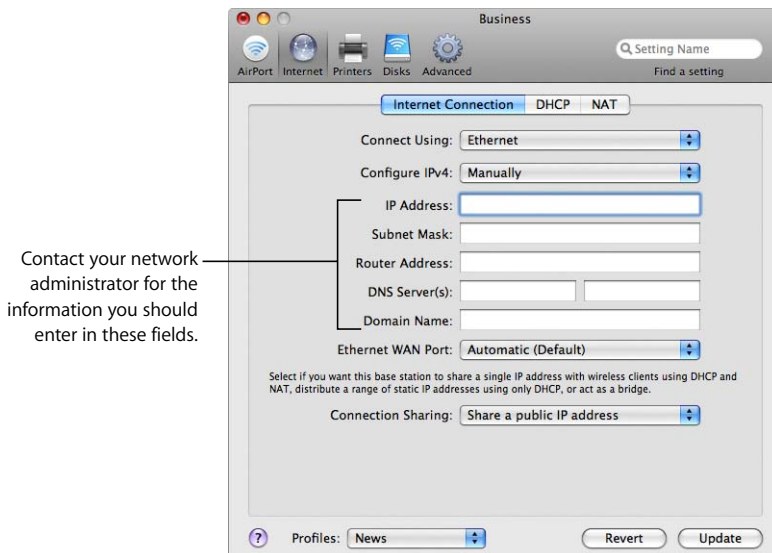
If you are using AirPort Utility to help you set up an Apple wireless device on an existing Ethernet network:

- 1 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer.
- 2 Click Continue and follow the onscreen instructions to connect to your local area network (LAN).

If you are using AirPort Utility to manually set up your wireless device:

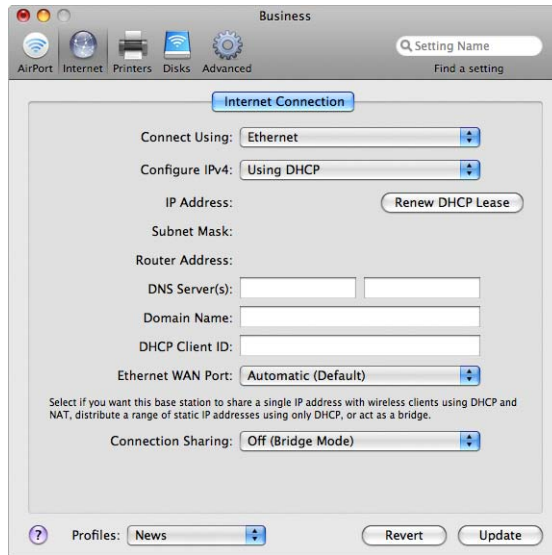
- 1 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer.
- 2 Select your device and choose Manual Setup from the Base Station menu, or double-click your device icon to open the configuration in a separate window.
- 3 Click Internet and choose Ethernet from the Connect Using pop-up menu.
- 4 Choose Manually or Using DHCP from the Configure IPv4 pop-up menu, depending on how IP addresses are provided on your Ethernet network. If you aren't sure, ask your service provider or network administrator.

If your addresses are provided manually, choose Manually from the Configure IPv4 pop-up menu. Enter your IP address information in the fields below the Configure IPv4 pop-up menu.



If you have already used AirPort Utility to set up your Apple wireless device, the fields below the Configure IPv4 pop-up menu may already contain the appropriate information.

If your IP address is provided by DHCP, choose Using DHCP from the Configure IPv4 pop-up menu.



- 5 Choose Off (Bridge Mode) from the Connection Sharing pop-up menu. Your wireless device “bridges” the Ethernet networks Internet connection to computers connected to the device wirelessly or by Ethernet.

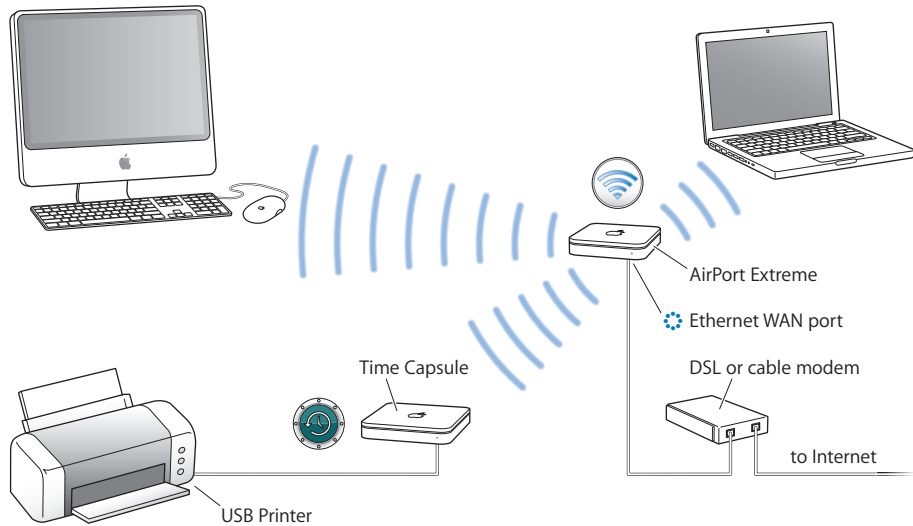
See “Setting Up Client Computers” on page 32 for information about how to set up client computers to connect to the Ethernet network.

Connecting Additional Devices to Your AirPort Extreme Network

Connect a USB printer to the USB port of your Apple wireless device (in this example, a Time Capsule) and everyone on the network can print to it. Connect a USB hub to the USB port of an AirPort Extreme Base Station or a Time Capsule, and then connect a hard disk and a printer so everyone on the network can access them.

If you connect a Time Capsule, you can use Time Machine in Mac OS X Leopard (v10.5.2 or later) to back up all of the Mac OS X Leopard computers on the network.

What It Looks Like



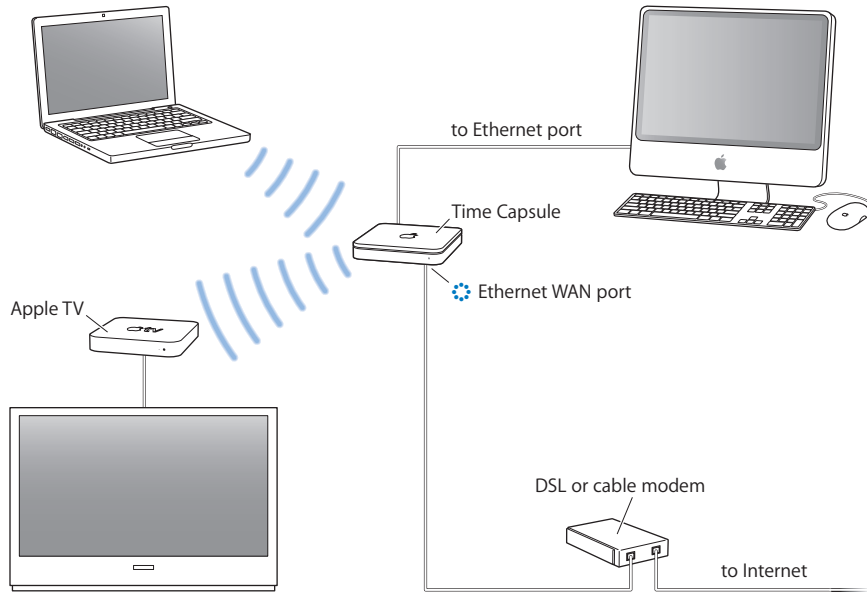
What to Do

Follow the instructions in the previous sections to set up your AirPort Extreme network depending on how you connect to the Internet or set up your wireless network. Connect a USB hard disk, printer, or hub to the USB port on your AirPort Extreme Base Station or Time Capsule.

Note: If you're using an AirPort Express in your network, you can connect a USB printer to the USB port, and everyone on the network can print to it. AirPort Express doesn't support connecting a USB hard disk.

Using Apple TV on Your AirPort Extreme Network to Play Content from iTunes

When you connect Apple TV to your AirPort Extreme network wirelessly, or using Ethernet, and then connect Apple TV to your widescreen TV, you can enjoy your favorite iTunes content including movies, TV shows, music and more. (See the documentation that came with your Apple TV for instructions setting it up.)



Setting Advanced Options

Connecting Additional Wireless Devices to Your AirPort Network

You can connect additional Apple wireless devices to extend the range of your wireless network. For example, you can connect an AirPort Extreme Base Station or a Time Capsule using Ethernet. A network with devices connected using Ethernet is known as a *roaming network*. You can also connect Apple wireless devices wirelessly. Connecting devices wirelessly creates what is known as a *Wireless Distribution System (WDS)*.

Setting Up Roaming

Several AirPort Extreme Base Stations or Time Capsules can be set up to create a single wireless network. Client computers using AirPort can move from device to device with no interruption in service (a process known as *roaming*).

To set up roaming:

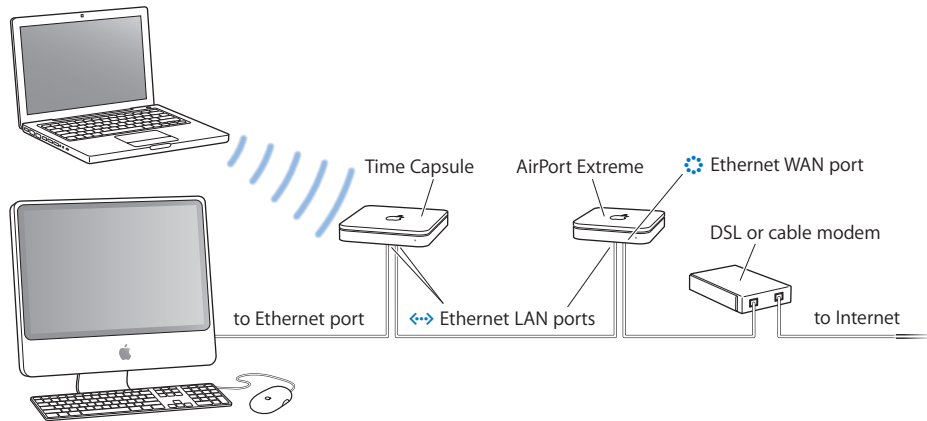
- 1 Connect all of the AirPort Extreme Base Stations and Time Capsules to the same subnet on your Ethernet network.
- 2 Give each device a unique name.

- 3 Give each device the same network name and password.
- 4 Set up the devices as bridges, following the instructions in the previous section.

If you want one device to assign IP addresses using DHCP, also do the following:

- 1 Set up one device to act as the DHCP server.
- 2 Set up the other devices as bridges, following the instructions in the previous section.

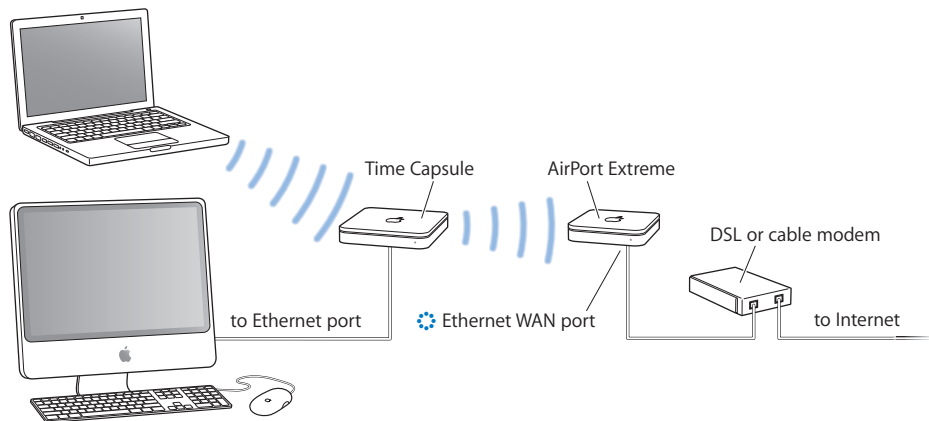
The device acting as a DHCP server can also receive its IP address via DHCP from a server on an Ethernet network or from a cable or DSL modem connected to an Internet service provider (ISP).



Setting Up a Wireless Distribution System (WDS)

When you connect devices wirelessly in a WDS, you set up each device as either a main, a remote, or a relay device.

You can connect AirPort Extreme 802.11n Base Stations or Time Capsules and use the 5 GHz frequency band in the network. Only client computers that have 802.11n wireless cards installed can join the network. If you want client computers using 802.11b or 802.11g wireless cards to join the network, set up the network using the 2.4 GHz frequency band, or add 802.11g AirPort Extreme or AirPort Express to the network. See “Choosing the Radio Mode” on page 21 for information about setting the frequency band of the network. You can also set up a dual-band network that utilizes both the 2.4 GHz and 5 GHz frequency bands, so client computers using 802.11n wireless cards can join the 5 GHz segment of the network, and computers using 802.11b or 802.11g wireless cards can join the 2.4 GHz segment. See “Setting up a Dual-Band (2.4 GHz and 5 GHz) Network” on page 48.



A main wireless device is connected to the Internet and shares its connection with remote and relay devices. A remote device shares the main device’s Internet connection. A relay device shares the main device’s Internet connection and transfers the connection to other remote or relay devices.

All three device configurations (main, remote, and relay) can also share the main device’s Internet connection with client computers wirelessly, or using Ethernet if the client computers are connected to the device by Ethernet.

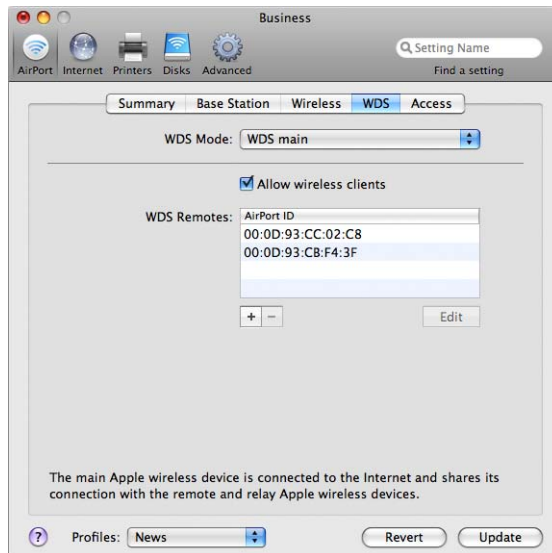
When you set up wireless devices in a WDS, you need to know the AirPort ID of each device. The AirPort ID is also known as the *MAC address*. To make it easier to set up a WDS, place all of the devices on a table and plug them into a power supply.

As part of the WDS setup process, you might consider giving all the devices unique names, to make them easier to identify in the future.

To set up the main wireless device to share its Internet connection with other wireless devices:

- 1 Click the AirPort status menu in the menu bar and choose the wireless network created by the device you want to set up as the main device.
- 2 Open AirPort Utility (located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer). Select the main device, and choose Manual Setup from the Base Station menu, or double-click the device's icon to open the configuration in a separate window. Enter the password if necessary. If the device is using the default password of *public*, you will not be prompted for a password.
- 3 Click the Wireless button, and then choose "Participate in a WDS network" from the Wireless Mode pop-up menu.
- 4 Click WDS and then choose "WDS main" from the WDS Mode pop-up menu.
- 5 Select the "Allow wireless clients" checkbox if you want client computers to connect to this device.
- 6 Click the Add (+) button and enter the MAC address of the wireless devices you want to connect to this main device.

If there is a device listed that you'd like to remove from the list, select it and click the Delete (–) button.



- 7 Click Update to send the new settings to the devices in the WDS.

By default, the “Allow wireless clients” checkbox is selected. If you deselect the checkbox and later want to change the settings on the wireless device, you must connect to the device’s LAN port with an Ethernet cable. You will not be able to connect to the device wirelessly.

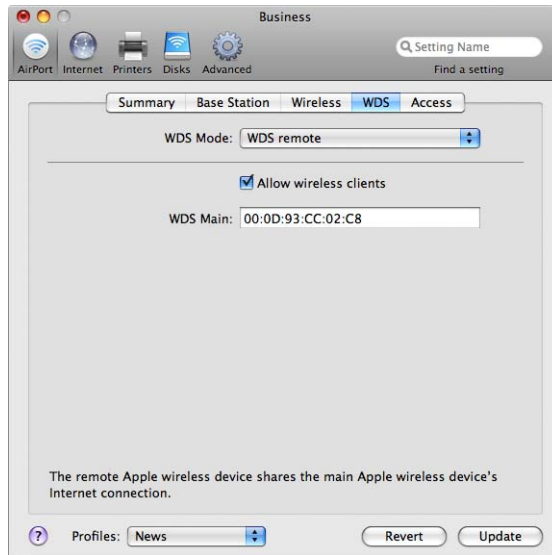
To set up additional remote devices to connect to the main device:

If you want to add additional remote or relay devices to the WDS after setting up the main and remote devices, use AirPort Utility again.

Remote devices need to be on the same channel as the main device. Before setting up additional remote devices, find the channel of the main device in the Summary pane of AirPort settings in AirPort Utility.

- 1 Click the AirPort status menu in the menu bar and choose the wireless network created by the device you want to set up as a remote device.
- 2 Open AirPort Utility (in the Utilities folder in the Applications folder on a Macintosh computer, or in Start > All Programs > AirPort on a computer using Windows). Select the remote device, and choose Manual Setup from the Base Station menu. Enter the password, if necessary. If the device is using the default password of *public*, you will not be prompted for a password.
- 3 Enter the same network password as the main device, if necessary.
- 4 Click the AirPort button, and then click Wireless. Choose “Participate in a WDS network” from the Wireless Mode pop-up menu, and choose the same channel as the device from the Channel pop-up menu.
- 5 Click WDS and choose “WDS remote” from the pop-up menu.

- 6 Enter the MAC address of the main device in the WDS Main field. The MAC address is also referred to as the AirPort ID and is printed on the label on the bottom of the device.



- 7 Click Update to transfer the settings.

By default, the "Allow wireless clients" checkbox is selected. If you deselect the checkbox and later want to change the settings on the wireless device, you must connect to the device's LAN port with an Ethernet cable. You will not be able to connect to the device wirelessly.

To set up a relay device to connect to the main device and share its connection with additional remote devices:

If you want to set up a relay device in the WDS to share its connection with other remote devices and wireless clients, use AirPort Utility again.

When you set up a relay, you also need to set up at least one additional remote to share the relay's connection. To set up a relay, first set it up as a remote by following the instructions on page 44.

Relay and remote devices need to be on the same channel as the main device. Before setting up a relay or remote device, find the channel of the main device in the Summary pane of AirPort settings in AirPort Utility.

- 1 Click the AirPort status menu in the menu bar to join the wireless network created by the wireless device you want to set up as the relay device.
- 2 Open AirPort Utility (in the Utilities folder in the Applications folder on a Macintosh computer, or in Start > All Programs > AirPort on a computer using Windows). Select the relay device, and choose Manual Setup from the Base Station menu. If the device is using the default password of *public*, you will not be prompted for a password.
- 3 Enter the same network password as the main device, if necessary.
- 4 Click the AirPort button, and then click Wireless. Choose “Participate in a WDS network” from the Wireless Mode pop-up menu, and choose the same channel as the main device from the Channel pop-up menu.
- 5 Click WDS and choose “WDS relay” from the WDS Mode pop-up menu.
- 6 Enter the MAC address of the main device in the Main AirPort ID field. The MAC address is also referred to as the AirPort ID and is printed on the label on the bottom of the device.
- 7 Click the Add (+) button and enter the AirPort ID of the remote device that this relay device will connect to.

If there is a device listed that you’d like to remove from the list, select it and click the Delete (–) button.

- 8 Click Update to transfer the new WDS settings to the relay and remote devices.

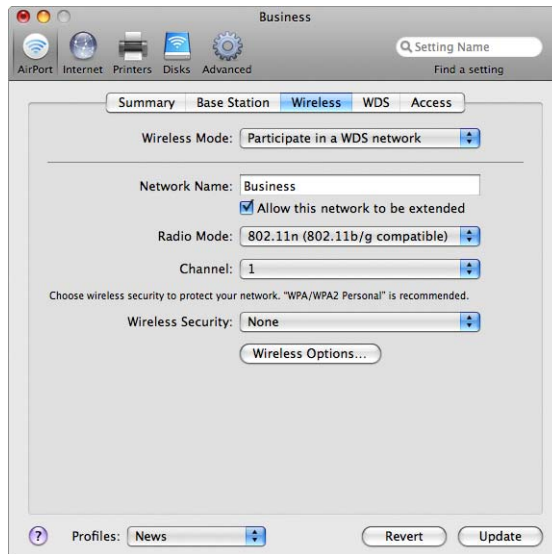
Extending the Range of an 802.11n Network

Extending the range of an 802.11n network is simpler if you are connecting another 802.11n device. Connecting two Apple 802.11n wireless devices makes the WDS setup process more straightforward.

To extend the range of an 802.11n network:

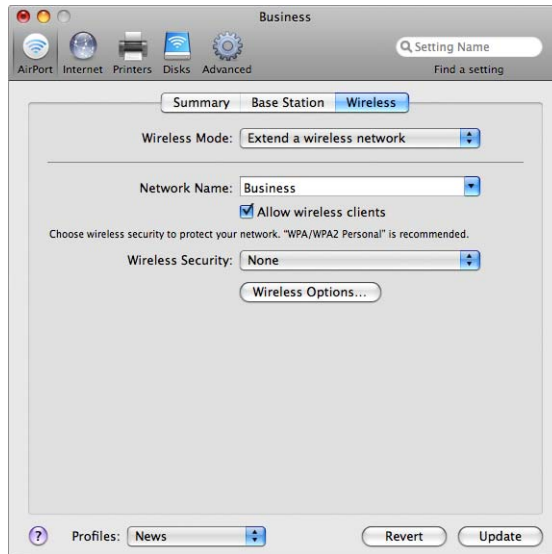
- 1 Open AirPort Utility and select the device that will connect to the Internet. See the previous sections of this document for instructions about setting up your wireless device, depending on your Internet connection.
- 2 Choose Manual Setup from the Base Station menu, or double-click the device’s icon to open the configuration in a separate window. Enter the password if necessary.
- 3 Click the AirPort button, and then click Wireless.

- 4 Choose “Create a wireless network” from the Wireless Mode pop-up menu, and then select the “Allow this network to be extended” checkbox.



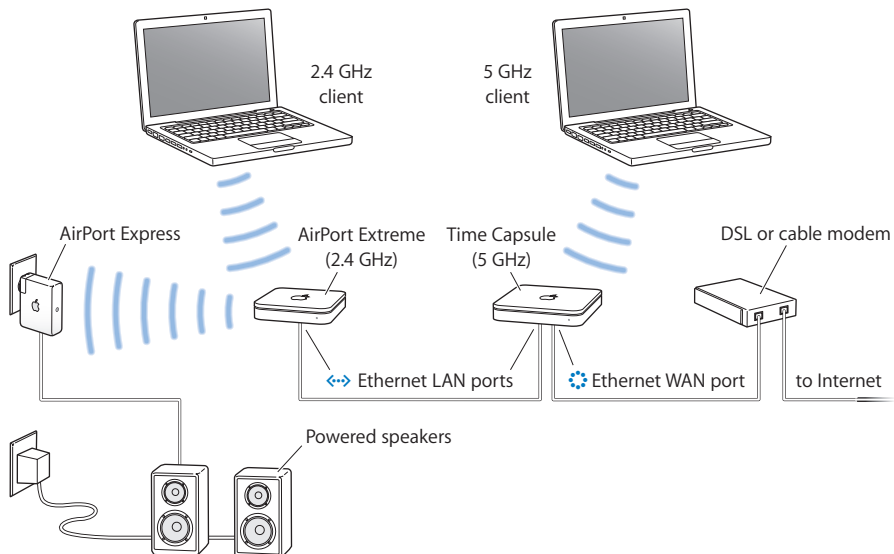
- 5 Next, select the device that will extend this network and choose Manual Setup from the Base Station menu, or double-click the device's icon to open its configuration in a separate window. Enter the password if necessary.
- 6 Choose “Extend a wireless network” from the Wireless Mode pop-up menu, and then choose the network you want to extend from the Network Name pop-up menu.
- 7 Enter the network name and password if necessary.

- 8 Click Update to update the device with new network settings.



Setting up a Dual-Band (2.4 GHz and 5 GHz) Network

You can set up a dual-band network that utilizes both the 2.4 GHz and 5 GHz frequency bands, so client computers using 802.11n wireless cards join the 5 GHz segment of the network, and computers using 802.11b or 802.11g wireless cards join the 2.4 GHz segment.



Setting up a dual-band network:

See “Choosing the Radio Mode” on page 21 for instructions about how to set up your Apple wireless device in the 5 GHz frequency range. Set up your device to connect to the Internet based on the type of service you use (DSL or cable modem service, or connecting to an existing Ethernet network that has Internet access). Give your 5 GHz network a name, such as Business 5G, so that 802.11n client computers can join the 5 GHz segment of the network.

Connect your 2.4 GHz Apple wireless device to your 802.11n device using Ethernet. Follow the instructions earlier in this chapter to set up your second device as a bridge. Give the 2.4 GHz segment of your network a different name, such as Business 2.4 so that 802.11b and 802.11g client computers can join the 2.4 GHz segment of the network.

In the previous illustration, an AirPort Express is connected to the 2.4 GHz segment of the network, so that 802.11b and 802.11g client computers can stream music to the AirPort Express using iTunes, while 5 GHz client computers can join the 5 GHz segment of the network created by the 802.11n AirPort Extreme Base Station.

Controlling the Range of Your AirPort Network

You can also shorten the range of your AirPort network. This might be useful if you want to control who has access to the network by restricting the range to a single room, for example.

To shorten the range of your AirPort network:

- 1 Open AirPort Utility (in the Utilities folder in the Applications folder on a Macintosh computer, or in Start > All Programs > AirPort on a computer using Windows).
- 2 Select your wireless device and choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 3 Click the AirPort button, and then click Wireless.
- 4 Click Wireless Options, and then choose a percentage setting from the Transmit Power pop-up menu. The lower the percentage, the shorter the range.

Keeping Your Network Secure

Your network is protected by the password you assign to it. However, you can take additional steps to help keep your network secure.

Networks managed by Simple Network Management Protocol (SNMP) may be vulnerable to denial-of-service attacks. Similarly, if you configure your wireless device over the WAN port, it may be possible for unauthorized users to change network settings. When remote configuration is enabled, the device’s Bonjour information (the device name and IP address) is published over the WAN port. Turning off remote configuration may provide additional security.

To help protect your network and wireless device:

- 1 Open AirPort Utility, select your device, and choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 2 Click the Advanced button, and then click Logging & SNMP.
- 3 Make sure the Allow SNMP Access and “Allow SNMP over WAN” checkboxes are not selected.

Using Wi-Fi Protected Access

AirPort Extreme supports WPA and WPA2 security standard for wireless networks. Using Mac OS X v10.3 or later or Windows XP with Service Pack 2, and 802.1X authentication capabilities, WPA security delivers more sophisticated data encryption than WEP, and also provides user authentication, which was virtually unavailable with WEP. If your computer has an AirPort Extreme wireless card installed, you can take advantage of the security updates in WPA2, including AES-CCMP encryption.

AirPort Extreme supports two modes of WPA and WPA2: Enterprise mode, which uses an authentication server for user authentication, and Personal mode, which relies on the capabilities of TKIP for WPA and AES-CCMP for WPA2, without requiring an authentication server.

Enterprise mode is designed for a larger network in which an IT professional is most likely setting up and managing the network. In order to set up a WPA or WPA2 Enterprise network, an 802.1X connection must be set up first in Network preferences on a Mac. To set up an 802.1x connection on a Windows computer, see the documentation that came with your computer. The 802.1X connection requires an authentication protocol, like TTLS, LEAP, or PEAP.

Setting up a WPA or WPA2 Enterprise network requires setting up an authentication server, such as a RADIUS server, to manage and validate network users' credentials, such as user names, passwords, and user certificates. See the documentation that came with the server to set it up.

Personal mode is for the home or small office network and can be set up and managed by most users. Personal mode does not require a separate authentication server. Network users usually need only enter a user name and password to join the network.

Note: If you change an existing WDS network from WEP to WPA, you will need to reset the wireless devices and set up your WDS again. For information about resetting your Apple wireless device, see the documentation that came with it.

To set up a WPA or WPA2 Enterprise network:

On a computer using Mac OS X, you first need to set up an 802.1x connection.

- 1 Open System Preferences, click Network, and then click AirPort.
- 2 Click Advanced, and then click 802.1X
- 3 Enter the settings for the connection.

Note: Some of the authentication protocols require digital certificate authorization on the server. See the documentation that came with your server to create and distribute digital certificates.

- 4 Click OK to save the connection settings.

To use AirPort Utility to set up a WPA or WPA2 Enterprise network on computers using Mac OS X and Windows XP:

- 1 Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 2 Choose WPA/WPA2 Enterprise, or WPA2 Enterprise from the Wireless Security pop-up menu, depending on the capabilities of the client computers that will join your network.
- 3 Click Configure RADIUS, and enter the IP address, port, and shared secret (or password) of the primary and secondary RADIUS authentication servers. Check with the administrator of the RADIUS server for information to type in these fields.

To set up a WPA or WPA2 Personal network:

- 1 Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 2 Choose WPA/WPA2 Personal or WPA2 Personal from the Wireless Security pop-up menu depending on the capabilities of the client computers that will join your network.
- 3 Type a password of 8 to 63 ASCII characters.

Setting Up Access Control

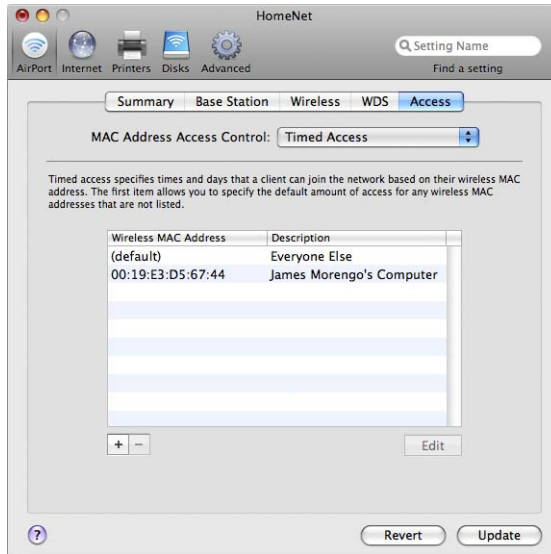
Access control lets you specify which computers can send or receive information through the wireless device to the wired network.

Each wireless-enabled computer has a unique MAC address. You can restrict access by creating an access control list that includes only the MAC addresses for computers you want to access your wired network.

To find the MAC address (AirPort ID) of your computer's AirPort Card, click the AirPort button in the Network pane of System Preferences.

To set up the access control list:

- 1 Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu. Enter the password if necessary.
- 2 Click the AirPort button, and then click Access.
- 3 Choose Timed Access or RADIUS from the MAC Address Access Control pop-up menu, depending on the device you're setting up.



- If you choose Timed Access, click the Add (+) button and enter the MAC address and description or name of the computers you are allowing to access the network. You can also click This Computer to add the MAC address and name of the computer you are using to set up this wireless device. Double-click the computer in the list and choose a value from each pop-up menu. Choose a day of the week or Everyday from the day pop-up menu, and then choose either “all day” or “between” from the other pop-up menu. If you choose “between,” you can edit the times of the day by double-clicking in the time fields.
- If you choose RADIUS, enter the type of RADIUS service, the RADIUS IP addresses, shared secret, and primary port for the primary RADIUS server. Enter the information for the secondary RADIUS server if there is one. Check with the server administrator if you don't have that information.

Important: AirPort access control prevents computers that aren't on the access control list from accessing the AirPort network. For information on how to prevent unauthorized computers from joining the AirPort network, see “Setting Up the AirPort Extreme Network” on page 17.

You can also add the MAC address of a third-party 802.11 wireless networking card to the access control list. Most third-party cards have the MAC address on a label attached to the metal case of the card.

Access control is not compatible with WPA or WPA2 Enterprise mode. You can use either access control or WPA Enterprise in a network, but you can't use both.

Using a RADIUS Server

Using a RADIUS server on your network lets you authenticate MAC addresses (AirPort IDs) on a separate computer, so that each device on the network doesn't need to store the MAC addresses of computers that have access to the network. Instead, all the addresses are stored on a server that is accessed through a specific IP address.

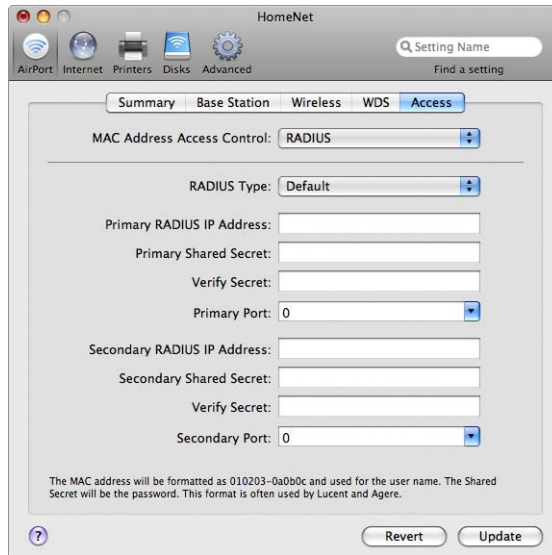
To set up authentication using a RADIUS server:

- 1 On the server, enter the MAC addresses of the computers that will access the network.
- 2 When the RADIUS server is set up, open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 3 Click AirPort, click Access, and then choose RADIUS from the MAC Address Access Control pop-up menu.
- 4 Choose a format from the RADIUS pop-up menu.

If you choose Default, your wireless device formats the MAC addresses as 010203-0a0b0c, and they are used as the user names on the RADIUS server. The shared secret is the password for users joining the network. This format is often used for Lucent and Agere servers.

If you choose Alternate, MAC addresses are formatted as 0102030a0b0c and are used for both the user name and password by users joining the network. This format is often used for Cisco servers.

- 5 Enter the IP address, port, and shared secret (or password) for the primary and secondary servers.



See the RADIUS documentation that came with your server, or check with the network administrator for more information on setting up the RADIUS server.

The access control list and RADIUS work together. When a user tries to join a network that authenticates using access control or a RADIUS server, the wireless device searches first in the access control list, and if the MAC address is there, the user can join the network. If the MAC address is not in the access control list, the device checks the RADIUS server for the MAC address. If it is there, the user can join the network.

Note: RADIUS access control is not compatible with WPA or WPA2 Personal mode. You can use either RADIUS access control or WPA Enterprise in a network, but you can't use both.

Directing Network Traffic to a Specific Computer on Your Network (Port Mapping)

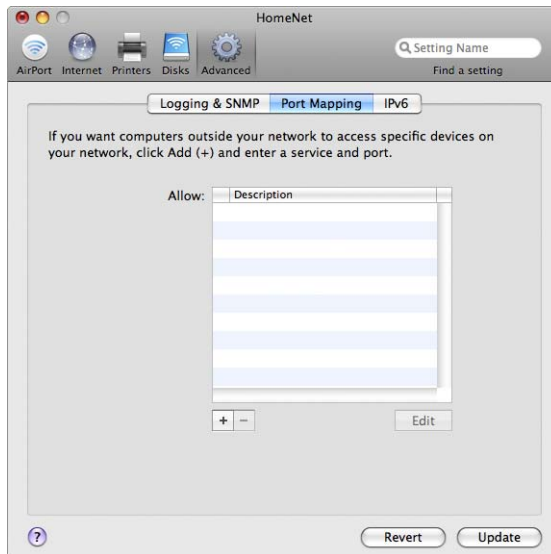
AirPort Extreme uses Network Address Translation (NAT) to share a single IP address with the computers that join the AirPort Extreme network. To provide Internet access to several computers with one IP address, NAT assigns private IP addresses to each computer on the AirPort Extreme network, and then matches these addresses with port numbers. The wireless device creates a port-to-private IP address table entry when a computer on your AirPort (private) network sends a request for information to the Internet.

If you are using a web, AppleShare, or FTP server on your AirPort Extreme network, other computers initiate communication with your server. Because the Apple wireless device has no table entries for these requests, it has no way of directing the information to the appropriate computer on your AirPort network.

To ensure that requests are properly routed to your web, AppleShare, or FTP server, you need to establish a permanent IP address for your server and provide inbound port mapping information to your Apple wireless device.

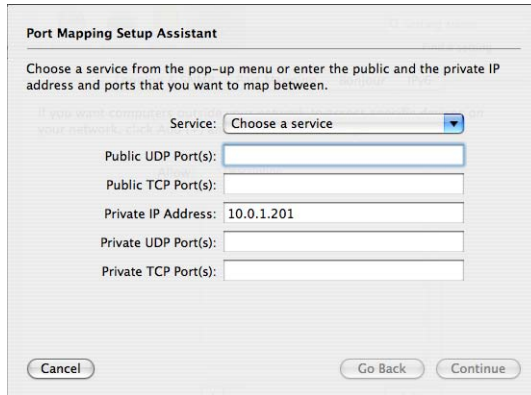
To set up inbound port mapping:

- 1 Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 2 Click the Advanced button, and then click Port Mapping.



- 3 Click the Add (+) button and choose a service, such as Personal File Sharing, from the Service pop-up menu.

Type any additional information you need in the text fields.

The image shows a 'Port Mapping Setup Assistant' dialog box. It has a title bar with the name 'Port Mapping Setup Assistant'. Below the title bar, there is a text area with the instruction: 'Choose a service from the pop-up menu or enter the public and the private IP address and ports that you want to map between.' Below this, there is a 'Service:' label followed by a dropdown menu with the text 'Choose a service'. Below the dropdown, there are six text input fields: 'Public UDP Port(s):', 'Public TCP Port(s):', 'Private IP Address:' (which contains the text '10.0.1.201'), 'Private UDP Port(s):', and 'Private TCP Port(s):'. At the bottom of the dialog, there are three buttons: 'Cancel', 'Go Back', and 'Continue'.

To use port mapping, you must configure TCP/IP manually on the computer that is running the web, AppleShare, or FTP server.

You can also set up a computer as a default host to establish a permanent IP address for the computer and provide inbound port mapping information to the AirPort Extreme Base Station or AirPort Express. This is sometimes known as a DMZ and is useful when playing some network games or videoconferencing.

To set up a default host:

- 1 Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 2 Click the Internet button, and then click NAT.
- 3 Select the "Enable Default Host at" checkbox. The default IP address is 10.0.1.253.
- 4 Enter the same IP address on the host computer.

Logging

You can set up your wireless device to log status information to the Mac OS X system log or the Syslog application on a Windows computer. This is helpful for understanding problems and monitoring a device's performance.

To set up logging:

- 1 Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 2 Click the Advanced button, and then click Logging and SNMP.

- 3 Enter the IP address of the computer that will receive the logs in the Syslog Destination Address field.
- 4 Choose a level from the Syslog Level pop-up menu.

You need to assign a Network Time Protocol (NTP) server for each wireless device, so the log information will contain the accurate time of the status logs.

To set the time automatically:

- 1 Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 2 Click the AirPort button, and then click Base Station.
- 3 Select the “Set time automatically” checkbox, and then choose an NTP server from the pop-up menu if you have access to one on your network or on the Internet.

If you click “Logs and Statistics” you can view and export logs, and view wireless client and DHCP client information.

If you export the logs, use the Mac OS X Console application, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer, to view the logs on the computer receiving them.

Setting up IPv6

IPv6 is a new version of Internet Protocol (IP). IPv6 is currently used primarily by some research institutions. Most computers do not need to set up or use IPv6.

The primary advantage of IPv6 is that it increases the address size from 32 bits (the current IPv4 standard) to 128 bits. An address size of 128 bits is large enough to support billions and billions of addresses. This allows for more addresses or nodes than are currently available. IPv6 also provides more ways to set up the address and simpler autoconfiguration.

By default, IPv6 is configured automatically, and the default settings are sufficient. However, if your network administrator or Internet service provider (ISP) has specifically told you to configure IPv6 manually, follow the instructions below.

Open AirPort Utility, select your wireless device, and then choose Manual Setup from the Base Station menu. Enter the password if necessary. Click the Advanced button, and then click IPv6.

To manually set IPv6 options:

- 1 Choose Node or Tunnel from the IPv6 mode pop-up menu, depending on the method you were instructed to use.

- 2 Choose Manually from the Configure IPv6 pop-up menu, and enter the information you were given from your ISP or network administrator.

Customizing the IPv6 firewall

If your wireless device supports it, you can use AirPort Utility to adjust IPv6 firewall settings.

To adjust IPv6 firewall settings:

- 1 Open AirPort Utility, located in the Utilities folder inside the Applications on a Mac, or in Start > All Programs > AirPort on a Windows computer.
- 2 Select your device from the list, and then enter the password.
- 3 Click the Advanced button, and then click IPv6 Firewall

By default, “Allow Teredo tunnels” and “Allow incoming IPSec authentication” are selected.

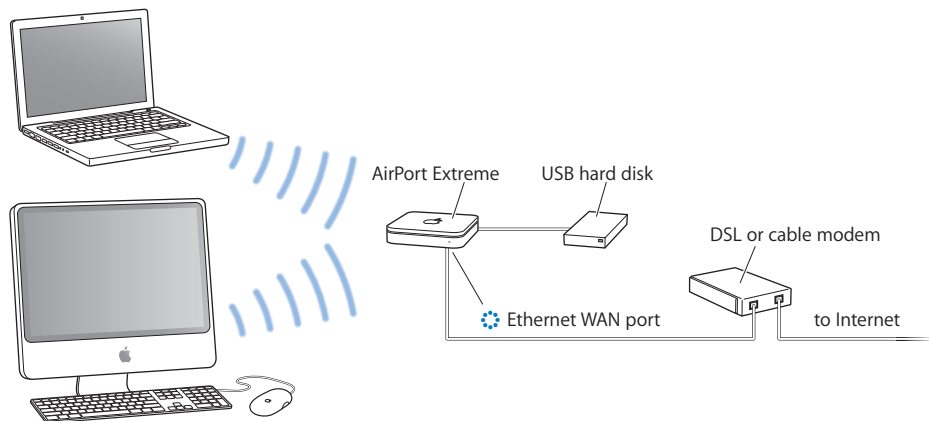
To provide access to specific devices on your network from outside the IPv6 firewall, click the Add (+) button and enter the IPv6 address and/or the port for the device.

To use an IPv6 firewall, you need an Apple 802.11n wireless device.

Sharing and Securing USB Hard Disks on Your Network

If you connect a USB hard disk to your AirPort Extreme Base Station or Time Capsule, computers connected to the network—both wireless and wired, Mac and Windows—can use it to back up, store, and share files.

If you’re using a Time Capsule, you don’t need to connect a hard disk to it. Every Time Capsule includes an internal AirPort disk.



To share a hard disk on you network:

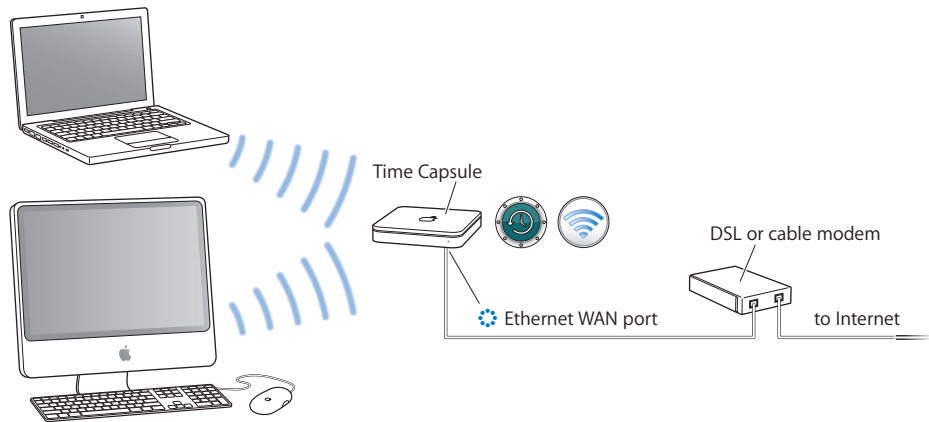
- 1 Plug the hard disk into the USB port on the back of the AirPort Extreme Base Station or Time Capsule.
- 2 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer.
- 3 Select your AirPort Extreme Base Station or your Time Capsule, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window. Enter the password if necessary.
- 4 Click the Disks button, and then click File Sharing.
- 5 Choose “With a disk password,” or “With base station password” if you want to secure the shared disk with a password, or choose “With accounts” if you want to secure the disk using accounts.
 - If you choose to use accounts, click Configure Accounts, click the Add (+) button, and then enter a name and password for each user that will access the disk.
- 6 Choose “Not allowed,” “Read only,” or “Read and write” to assign guest access to the disk.
- 7 Select the “Share disks over Ethernet WAN port” checkbox if you want to provide remote access to the disk over the WAN port.

Data transfer speed may vary, depending on the network.

Using a Time Capsule in Your Network

If you're using a Time Capsule and a computer with Mac OS X Leopard (v10.5.2 or later), you can use Time Machine to automatically back up all of the computers on the network that are using Leopard. Other Mac computers and Windows computers can access the Time Capsule's internal AirPort disk to back up, store, and share files.

And because every Time Capsule is also a full-featured 802.11n base station, you can set up your Time Capsule to share an Internet connection with computers on the AirPort network it creates.



For information about using your Time Capsule with Time Machine in Mac OS X Leopard, search for “Time Capsule” in Mac Help.

Connecting a USB Printer to an Apple Wireless Device

You can connect a compatible USB printer to your Apple wireless device (an AirPort Extreme Base Station, AirPort Express, or Time Capsule), so that anyone on the network using Mac OS X v10.2.3 or later, Windows XP with Service Pack 2, or Windows Vista can print to that printer.

To use a printer on your network:

- 1 Connect the printer to the USB port on the Apple wireless device.
- 2 Set up the client computers:
 - On a computer using Mac OS X v10.5 or later, open System Preferences and click Print & Fax. Select the printer from the Printers list. If the printer isn't in the list, click Add (+) at the bottom of the list, locate the printer, and then click Add.

- On a computer using Mac OS X v10.2.3 or later, open Printer Setup Utility located in the Utilities folder in the Applications folder, and then select the printer from the list. If the printer is not in the list, click Add, choose Bonjour from the pop-up menu, and then select the printer from the list.
- On a computer using Windows, install Bonjour for Windows from AirPort Utility CD, and follow the onscreen instructions to connect to the printer.

You can change the name of the printer from the default name to one you choose.

To change the name of your USB printer:

- 1 Open AirPort Utility, select your device, and then choose Manual Setup from the Base Station menu, or double-click the device icon to open its configuration in a separate window.
- 2 Click the Printer button and type a name for the printer in the USB Printers field.

Adding a Wireless Client to Your 802.11n Network

If your Apple wireless device supports it, and your network is password-protected using WPA Personal or WPA/WPA2 Personal, you can provide wireless clients access to your network without requiring them to enter the network password.

When you allow a client access to your network, the client's name and wireless MAC address (or AirPort ID) are stored in the access control list of AirPort Utility until you remove them from the list. You can provide 24 hours of access, after which time the client will no longer be able to access your network.

When you provide a client access to your wireless network, the client does not need to enter the network password.

To allow client access to your network:

- 1 Open AirPort Utility, located in the Utilities folder in the Applications folder on a Mac, or in Start > All Programs > AirPort on a Windows computer.
- 2 Select your Apple wireless device and choose Manual Setup from the Base Station menu. Enter the password if necessary.
- 3 Choose Add Wireless Clients from the Base Station menu.
- 4 Select how you want the client to access the network:
 - Select PIN to enter the eight-digit number provided by the client requesting network access.
 - Select "First attempt" to allow network access to the first client attempting to join the network.
 - Select "Limit client's access to 24 hours" if you want to provide only one day of access to your network. If you don't select this option, the client will have access to your network until you remove the name from the list.

Solving Problems

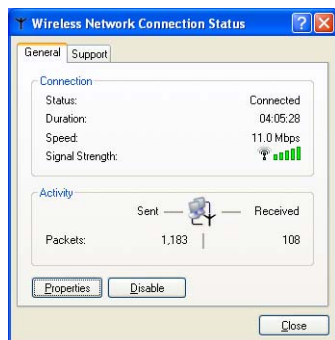
If you have trouble connecting to the Internet with any AirPort Extreme network design, try the following:

On a computer using Mac OS X:

- Make sure the wireless device is connected to the Internet. The computers on your AirPort network cannot connect to the Internet if your device is not connected to the Internet.
- Check your Internet connection using your computer. If you can't connect with your computer, the problem may be with your Internet connection.
- On a Mac using Mac OS X v10.5, check the active network services in the Network pane of System Preferences. Make sure the ports you want to use are active.
- Open Network preferences and then click AirPort. Make sure that the computer has joined the AirPort network created by your wireless device.
- Restart your computer. This renews the IP address you receive from the wireless device. The IP addresses should be in the range of 10.0.1.2 to 10.0.1.200, 172.16.1.2 to 172.16.1.200, or 192.168.1.2 to 192.168.1.200, depending on the address scheme the wireless device uses.
- If the wireless device is set up as a DHCP server, make sure you choose "Share a public IP address" from the Connection Sharing pop-up menu on the Internet Connection pane of Internet settings in AirPort Utility.
- If you are using a cable modem and your wireless device cannot connect to the Internet, turn off the cable modem, wait a few minutes, and then turn it on again.

On a computer using Windows:

- Make sure the wireless device is connected to the Internet. The computers on your AirPort network cannot connect to the Internet if your device is not connected to the Internet.
- Check your Internet connection using your computer. If you can't connect with your computer, the problem may be with your Internet connection.
- Right-click the wireless connection icon, and then choose Status.



- Make sure that the computer has joined the AirPort network created by your wireless device.
- Restart your computer. This renews the IP address you receive from the wireless device. The IP addresses should be in the range of 10.0.1.2 to 10.0.1.200, 172.16.1.2 to 172.16.1.200, or 192.168.1.2 to 192.168.1.200 depending on the address scheme the device uses.
- If the device is set up as a DHCP server, make sure the “Obtain an IP address automatically” checkbox is selected in the General pane of Internet Protocol (TCP/IP) Properties. Right-click the wireless connection icon and click Properties. Click Internet Protocol (TCP/IP), and then click Properties.

More Information About AirPort

You can find more information about AirPort in the following locations:

- **AirPort Utility Help**

Look in AirPort Utility Help for information on setting up an AirPort Extreme network; using an AirPort Extreme Base Station, an AirPort Express, or a Time Capsule; editing settings; avoiding sources of interference; locating additional information on the Internet; and more. On a computer using Mac OS X, open AirPort Utility and choose AirPort Utility Help from the Help menu. On a computer using Windows, open AirPort Utility and click Help.

- **World Wide Web**

Apple AirPort website at www.apple.com/airportextreme

Apple Support website at www.apple.com/support/airport

This chapter defines terms and concepts used to discuss computer networks. Use it as a reference to help you understand what is taking place behind the scenes of your AirPort wireless network.

Basic Networking

Packets and Traffic

Information travels across a network in chunks called packets. Each packet has a header that tells where the packet is from and where it's going, like the address on the envelope when you send a letter. The flow of all these packets on the network is called traffic.

How Information Reaches Its Destination

Hardware Addresses

Your computer “listens” to all of the traffic on its local network and selects the packets that belong to it by checking for its hardware address (also called the *media access control*, or *MAC address*) in the packet header. This address is a number unique to your computer.

Every hardware product used for networking is required to have a unique hardware address permanently embedded in it. Your AirPort Card's number is called the AirPort ID.

IP Addresses

Since the Internet is a network of networks (connecting millions of computers), hardware addresses alone are not enough to deliver information on the Internet. It would be impossible for your computer to find its packets in all the world's network traffic, and impossible for the Internet to move all traffic to every network.

So, your computer also has an Internet Protocol (IP) address that defines exactly where and in what network it's located. IP addresses ensure that your local Ethernet network receives only the traffic intended for it. Like the hierarchical system used to define zip codes, street names, and street numbers, IP addresses are created according to a set of rules, and their assignment is carefully administered.

The hardware address is like your name; it uniquely and permanently identifies you. But it doesn't offer any clues about your location, so it's only helpful in a local setting. An IP address is like your street address, which contains the information that helps letters and packages find your house.

Rules for Sending Information (Protocols)

A protocol is a set of rules that define how communication takes place. For instance, a networking protocol may define how information is formatted and addressed, just as there's a standard way to address an envelope when you send a letter.

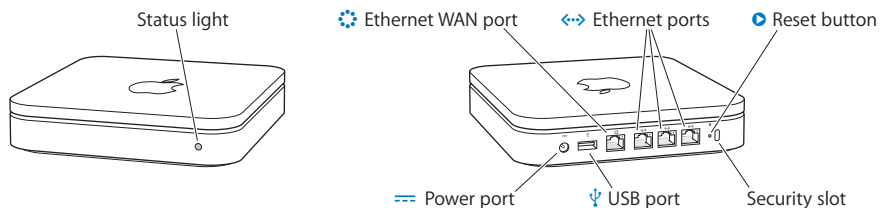
Using the AirPort Extreme Base Station

This section describes the different network interfaces of the AirPort Extreme Base Station and describes the functions the base station can provide.

Base Station Interfaces

To use the AirPort Extreme Base Station, you configure how its networking interfaces will be used. The AirPort Extreme Base Station has five hardware networking interfaces:

- **AirPort interface:** The AirPort interface creates an AirPort network for AirPort-enabled computers to join. The base station can provide IP services such as DHCP and NAT using this interface. The base station cannot use the AirPort interface to establish a connection with the Internet.
- **Ethernet WAN (⚙️) interface:** The Ethernet WAN interface is used to connect DSL or cable modems and connect to the Internet.
- **Ethernet LAN (↔️) interface:** If your base station has one or more Ethernet LAN interface ports, you can use them to provide IP services to local Ethernet clients.
- **USB (🔌) interface:** The USB interface is used to connect a USB printer to the AirPort Extreme Base Station.



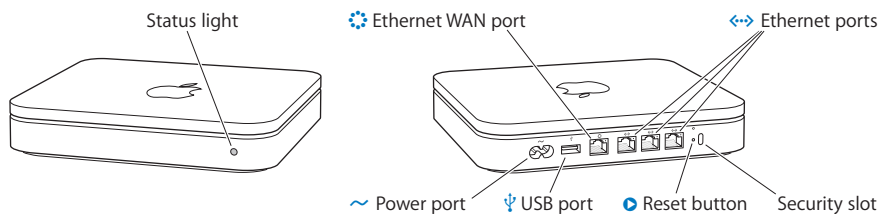
Using the Time Capsule

This section describes the different network interfaces of the Time Capsule and describes the functions it can provide.

Time Capsule Interfaces

To use your Time Capsule, you configure how its networking interfaces will be used. The Time Capsule has five hardware networking interfaces:

- **AirPort interface:** The AirPort interface creates an AirPort network for AirPort-enabled computers to join. The Time Capsule can provide IP services such as DHCP and NAT using this interface. It cannot use the AirPort interface to establish a connection with the Internet.
- **Ethernet WAN (⚡) interface:** The Ethernet WAN interface is used to connect DSL or cable modems and connect to the Internet.
- **Ethernet LAN (↔) interface:** The Time Capsule has three Ethernet LAN interface ports. You can use them to provide IP services to local Ethernet clients.
- **USB (ψ) interface:** The USB interface is used to connect a USB printer to the AirPort Extreme Base Station.



Using the AirPort Express

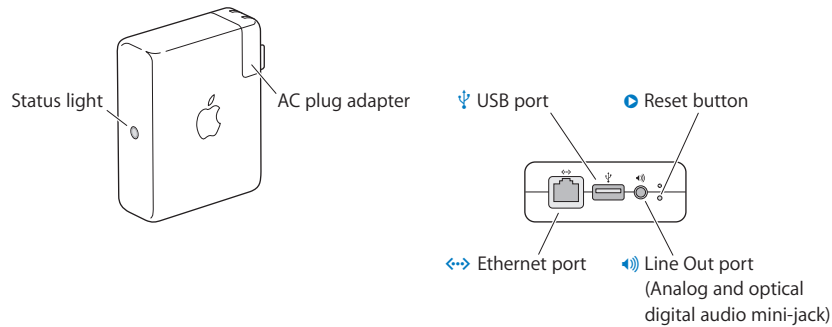
This section describes the different network interfaces of the AirPort Express Base Station and describes the functions the base station can provide.

AirPort Express Interfaces

To set up the AirPort Express Base Station, you configure how its networking interfaces will be used. The AirPort Express Base Station has four hardware networking interfaces:

- **AirPort interface:** The AirPort interface creates an AirPort network for AirPort-enabled computers to join. The base station can provide IP services such as DHCP and NAT using this interface. The base station cannot use the AirPort interface to establish a connection with the Internet.
- **Ethernet WAN (⚡) interface:** Use the Ethernet WAN interface to connect DSL or cable modems and connect to the Internet.
- **USB (ψ) interface:** Use the USB interface to connect a USB printer to the AirPort Extreme Base Station.

- **Audio (🔊) interface:** Use the analog and optical digital audio stereo mini-jack to connect an AirPort Express to a home stereo or powered speakers.



Apple Wireless Device Functions

- **Bridge:** Each Apple wireless device is configured by default as a bridge between the wireless AirPort network and the wired Ethernet network. Connecting an AirPort network to an Ethernet network through the device's Ethernet LAN port (↔), bridges the wireless AirPort network to the wired Ethernet network.

Important: If you are connecting an Ethernet network to the device's Ethernet LAN port (↔), make sure the Ethernet network does not have an Internet connection.

- **NAT router:** One of the most powerful features of Apple wireless devices is their ability to share one Internet connection with several computers. To provide this service, the device acts as a router. The device can be configured to provide both bridging services and routing services at the same time.
- **DHCP server:** When you configure the wireless device to act as a DHCP server, it provides IP addresses to both wired and wireless client computers that are configured to obtain IP addresses using DHCP. Using DHCP makes IP configuration simple for client computers, since they don't need to enter their own IP information.

Items That Can Cause Interference with AirPort

The farther away the interference source, the less likely it is to cause a problem. The following items can cause interference with AirPort communication:

- Microwave ovens
- DSS (Direct Satellite Service) radio frequency leakage
- The original coaxial cable that came with certain types of satellite dishes. Contact the device manufacturer and obtain newer cables.
- Certain electrical devices, such as power lines, electrical railroad tracks, and power stations

- Cordless telephones that operate in the 2.4 gigahertz (GHz) range. If you have problems with your phone or AirPort communication, change the channel of your base station.
- Other AirPort and wireless networks
- Adjacent base stations using nearby channels. If base station A is set to channel 1, base station B should be set to channel 6 or 11. For best results, use channels 1, 6, or 11 when operating your base station in the 2.4 GHz range.
- Moving objects that temporarily place metal between your computer and the base station

10Base-T The most common cabling method for Ethernet. 10Base-T conforms to IEEE standard 802.3. It was developed to enable data communications over unshielded twisted pair (telephone) wiring at speeds of up to 10 megabits per second up to distances of approximately 330 feet on a network segment.

10/100Base-T A networking standard that supports data transfer rates up to 100 Mbps (100 megabits per second). Because it is 10 times faster than Ethernet, it is often referred to as Fast Ethernet.

10/100/1000Base-T A term describing various technologies for transmitting Ethernet packets at a rate of a gigabit per second. Sometimes referred to as Gigabit Ethernet. In 2000, Apple's Power Mac G4 and PowerBook G4 were the first mass-produced personal computers featuring the 10/100/1000Base-T connection. It quickly became a built-in feature in many other computers.

802.11a An IEEE standard for a wireless network that operates at 5 GHz with rates up to 54 Mbps.

802.11b An IEEE standard for a wireless network that operates at 2.4 GHz with rates up to 11 Mbps.

802.11g An IEEE standard for a wireless network that operates at 2.4 GHz Wi-Fi with rates up to 54 Mbps.

802.11n A task group of the IEEE 802.11 committee whose goal is to define a standard for high throughput speeds of at least 100 Mbps on wireless networks. Some proposals being fielded by the task group include designs for up to 540 Mbps. multiple-input multiple-output (MIMO) technology, using multiple receivers and multiple transmitters in both the client and access point to achieve improved performance is expected to form the basis of the final specification. See Mbps, MIMO.

access point Also known as a *wireless access point* (WAP), a device that connects wireless devices together to form a network.

authentication The process that occurs after association to verify the identity of the wireless device or end user and allow access to the network. See WPA, WPA2.

backbone The central part of a large network that links two or more subnetworks. The backbone is the primary data transmission path on large networks such as those of enterprises and service providers. A backbone can be wireless or wired.

bandwidth The maximum transmission capacity of a communications channel at any point in time. Bandwidth, usually measured in bits per second (bps), determines the speed at which information can be sent across a network. If you compare the communications channel to a pipe, bandwidth represents the pipe width and determines how much data can flow through the pipe at any one time. The greater the bandwidth, the faster data can flow. See bps.

base station In the area of wireless computer networking, a base station is a radio receiver/transmitter that serves as the hub of the local wireless network, and may also be the gateway between a wired network and the wireless network. A base station can also be referred to as an access point or router.

Bluetooth A technology designed for short-range, wireless communications among computing devices and mobile products, including PCs and laptop computers, personal digital assistants, printers, and mobile phones. Designed as a cable replacement, Bluetooth enables short-range transmission of voice and data in the 2.4 GHz frequency spectrum within a range of about 30 feet.

bps Bits per second. A measure of data transmission speed across a network or communications channel; bps is the number of bits that can be sent or received per second. It measures the speed at which data is communicated and should not be—but often is—confused with bytes per second. Whereas “bits” is a measure of transmission speed, “bytes” is a measure of storage capacity. See bandwidth, Mbps.

bridge A wireless device that connects multiple networks together. Using an access point as a bridge turns off Network Address Translation (NAT) and DHCP routing and simply extends the range of service.

broadband A comparatively fast Internet connection possessing sufficient bandwidth to accommodate multiple voice, data, and video channels simultaneously. Cable, DSL, and satellite are all considered to be broadband channels; they provide much greater speed than dial-up Internet access over telephone wires. See cable modem, DSL.

broadband modem A device that connects a local computer or network to a high-speed Internet service, such as DSL or Cable Internet. See cable modem, DSL.

cable modem A device used with broadband Internet service provided by a traditional cable TV service. Cable modems convert analog data from the cable TV system into a digital format that can be used by a computer. See broadband modem.

channel One portion of the available radio spectrum that all devices on a wireless network use to communicate. Changing the channel on the access point/router can help reduce interference.

client Any computer or device connected to a network that requests files and services (files, print capability) from the server or other devices on the network. The term also refers to end users.

DHCP Dynamic Host Configuration Protocol. A protocol for dynamically assigning IP addresses from a predefined list to nodes on a network. When they log on, network nodes automatically receive an IP address from a pool of addresses served by a DHCP. The DHCP server provides (or leases) an IP address to a client for a specific period of time. The client will automatically request a renewal of the lease when the lease is about to run out. If a lease renewal is not requested and it expires, the address is returned to the pool of available IP addresses. Using DHCP to manage IP addresses simplifies client configuration and efficiently utilizes IP addresses. See IP address.

DNS Domain Name System. An Internet service that translates alphanumeric domain names to assigned IP addresses and vice versa. The term is typically used to describe the server that makes the translation. Every website has its own specific IP address on the Internet. DNS typically refers to a database of Internet names and addresses that translates the alphanumeric names to the official Internet Protocol numbers and vice versa. For instance, a DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. See IP, IP address.

DSL Digital Subscriber Line. A dedicated digital circuit between a residence or business and a telephone company's central office. It allows high-speed data, voice, and video transmissions over existing twisted-pair copper plain old telephone service (POTS) telephone wires. See broadband.

dual-band A device that is capable of operating in either of two frequencies. On a wireless network, dual-band devices are capable of operating in the 2.4 GHz (802.11b/g) or 5 GHz (802.11a) bands.

encryption A mechanism for providing data confidentiality. See WPA, WPA2.

Ethernet The most popular international standard technology for wired local area networks (LANs). It provides from 10 Mbps transmission speeds on basic 10Base-T Ethernet networks to 100 Mbps transmission speeds on Fast Ethernet networks, 1000 Mbps on Gigabit Ethernet, and 10,000 Mbps on 10 Gigabit Ethernet.

firewall A system of software and/or hardware that resides between two networks to prevent access by unauthorized users. The most common use of a firewall is to provide security between a local network and the Internet. Firewalls can make a network appear invisible to the Internet and can block unauthorized and unwanted users from accessing files and systems on the network. Hardware and software firewalls monitor and control the flow of data in and out of computers in both wired and wireless enterprise, business and home networks. They can be set to intercept, analyze, and stop a wide range of Internet intruders and hackers.

gateway In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, and so on.

hotspot A location where users can access the Internet using Wi-Fi laptops and other Wi-Fi enabled devices. Access may be provided free or for a fee. Hotspots are often found at coffee shops, hotels, airport lounges, train stations, convention centers, gas stations, truck stops and other public meeting areas. Corporations and campuses often offer it to visitors and guests. Hotspot service is sometimes available aboard planes, trains, and boats.

hub A multiport device used to connect client devices to a wired Ethernet network. Hubs can have numerous ports and can transmit data at speeds ranging from 10 to 1000 Mbps to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more. See router.

IEEE 802.11 The family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 committee, which establishes standards for wireless Ethernet networks. 802.11 standards define the over-the-air interface between wireless clients and a base station, or access point that is physically connected to the wired network.

IP Internet Protocol. The basic communications protocol of the Internet. See IP address, TCP/IP.

IP address Internet Protocol address. IP Version 4, the most widely used Internet protocol, provides a 32-bit number that identifies the sender or receiver of information sent across the Internet. An IP address has two parts: The identifier of the particular network on the Internet and the identifier of the particular device (which can be a server or a workstation) within that network. The newer IP, Version 6, provides a 128-bit addressing scheme to support a much greater number of IP addresses. See DHCP, DNS, IP.

IP subnet An IP subnet is a local network as defined by IP network numbers. Connecting to a subnet involves connecting to the appropriate hardware network and configuring IP for that network.

LAN Local area network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files, and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN. See WAN.

MAC address Media Access Control address. A unique hardware number that identifies each device on a network. A device can be a computer, printer, and so on. A MAC address is also known as an AirPort ID.

Mbps Megabits per second. A measurement of data speed equivalent to a million bits per second.

MIMO Multiple-input multiple-output. An advanced signal processing technology that uses multiple receivers and multiple transmitters in both the client and access point to achieve data throughput speeds of 100 Mbps. See 802.11n.

NAT Network Address Translation. A network capability that enables multiple computers to dynamically share a single incoming IP address from a dial-up, cable, or DSL connection. NAT takes a single incoming public IP address and translates it to a new private IP address for each client on the network. See DHCP, IP address.

network name A name used to identify a wireless network. See SSID.

NIC Network interface card. A wireless or wired PC adapter card that allows the client computer to utilize network resources. Most office-wired NICs operate at 100 Mbps. Wireless NICs operate at data rates defined by 802.11 standards.

packet A unit of information transmitted from one device to another on a network. A packet typically contains a header with addressing information, data, and a checksum to ensure data integrity.

pass phrase A series of characters used to create a key that is used by Wi-Fi Protected Access (WPA). See PSK, WPA.

print server A network device, often a computer, that connects to at least one printer, allowing it to be shared among computers on a network.

PSK Pre-shared key. A mechanism in Wi-Fi Protected Access (WPA)-Personal that allows the use of manually entered keys or passwords to initiate WPA security. The PSK is entered on the access point or home wireless gateway and each PC that is on the Wi-Fi network. After entering the password, Wi-Fi Protected Access automatically takes over. It keeps out eavesdroppers and other unauthorized users by requiring all devices to have the matching password. The password also initiates the encryption process which, in WPA is Temporal Key Integrity Protocol (TKIP) and in WPA2 is Advanced Encryption Standard (AES). See TKIP, WPA-Personal, WPA2-Personal.

roaming (Wi-Fi) The ability to move from one area of Wi-Fi coverage to another with no loss in connectivity (hand-off).

router A wireless router is a device that accepts connections from wireless devices to a network, includes a network firewall for security, and provides local network addresses. See hub.

server A computer that provides resources or services to other computers and devices on a network. Types of servers include print servers, Internet servers, mail servers, and DHCP servers. A server can also be combined with a hub or router. See DHCP, hub, router.

SSID Service set identifier. A unique 32-character network name, or identifier, that differentiates one wireless LAN from another. All access points and clients attempting to connect to a specific WLAN must use the same SSID. The SSID can be any alphanumeric entry up to a maximum of 32 characters. See network name.

subnet An IP address range that is part of a larger address range. Subnets are used to subdivide a network address of a larger network into smaller networks. Subnets connect to other networks through a router. Each individual wireless LAN will typically use the same subnet for all of its clients. See IP address, router.

TCP Transmission Control Protocol. The transport-level protocol used with the Internet Protocol (IP) to route data across the Internet. See IP, TCP/IP.

TCP/IP The underlying technology of Internet communications. While IP handles the actual delivery of data, TCP tracks the data packets to efficiently route a message through the Internet. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup (see DHCP) or permanently assigned as a static address. All TCP/IP messages contain the address of the destination network, as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide. For example, when a user downloads a web page, TCP divides the page file on the web server into packets, numbers the packets, and forwards them individually to the user's IP address. The packets may be routed along different paths before reaching the user's address. At the destination, TCP reassembles the individual packets, waiting until they have all arrived to present them as a single file. See IP, IP address, packet, TCP.

throughput Usually measured in bps, Kbps, Mbps or Gbps, throughput is the amount of data that can be sent from one location to another in a specific amount of time. See bps, Mbps.

USB Universal Serial Bus. A high-speed bidirectional serial connection used to transfer data between a computer and peripherals such as digital cameras and memory cards.

WEP Wired equivalent privacy. The original security standard used in wireless networks to encrypt the wireless network traffic. See WPA, Wireless local area network

Wi-Fi A term developed by the Wi-Fi Alliance to describe wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers.

Wi-Fi Certified The certification standard designating IEEE 802.11-based wireless local area network (WLAN) products that have passed interoperability testing requirements developed and governed by the Wi-Fi Alliance.

wireless network Devices connected to a network using a centralized wireless access point. See WLAN.

WLAN (WLAN). A data communications network that spans large local, regional, national or international areas and is usually provided by a public carrier (such as a telephone company or service provider). The term is used to distinguish between phone-based data networks and Wi-Fi networks. Phone networks are considered wide area networks (WANs) and Wi-Fi networks are considered wireless local area networks (WLANs). See LAN.

WPA - Enterprise Wi-Fi Protected Access-Enterprise. A wireless security method that provides strong data protection for multiple users and large managed networks. It uses the 802.1X authentication framework with TKIP encryption and prevents unauthorized network access by verifying network users through an authentication server. See 802.1X.

WPA - Personal Wi-Fi Protected Access-Personal. A wireless security method that provides strong data protection and prevents unauthorized network access for small networks. It uses TKIP encryption and protects against unauthorized network access.

WPA2 Wi-Fi Protected Access 2. The follow-on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the ratified IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1X-based authentication. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA. Like WPA, WPA2 uses the 802.1X/EAP framework as part of the infrastructure that ensures centralized mutual authentication and dynamic key management and offers a pre-shared key for use in home and small office environments. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multiband and multimode. See WPA2-Enterprise, WPA2-Personal.

WPA2 - Enterprise Wi-Fi Protected Access 2 - Enterprise. The follow-on wireless security method to WPA that provides stronger data protection for multiple users and large managed networks. It prevents unauthorized network access by verifying network users through an authentication server. See WPA2.

WPA2 - Personal Wi-Fi Protected Access 2 - Personal. The follow-on wireless security method to WPA that provides stronger data protection and prevents unauthorized network access for small networks. See WPA2, PSK.

www.apple.com/airportextreme
www.apple.com/airport

© 2008 Apple Inc. All rights reserved.

Apple, the Apple logo, AirPort, AirPort Extreme, AppleShare, AppleTalk, Bonjour, Mac, and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries. AirPort Express, AirTunes, Time Capsule, and Time Machine are trademarks of Apple Inc. Other product and company names mentioned herein may be trademarks of their respective companies.

019-1155