Managing AirPort Extreme Networks

Includes information and instructions for planning, setting up, and managing AirPort Extreme networks

Contents

About This Guide

This guide provides information about planning a large-scale AirPort network, as well as instructions on using AirPort Client Monitor and AirPort Management Utility.

The guide will help you design, plan, set up, manage, and monitor large-scale AirPort wireless networks using AirPort Client Monitor, AirPort Management Utility, and the network components of Mac OS X.

The guide makes the following assumptions:

- You have an understanding of the network features of Mac OS X v10.2 and later.
- You have a working knowledge of AirPort Admin Utility and a general understanding of how to set up and manage an AirPort wireless network.
- You have administrative access to your network.

If you need more background information about AirPort and the network features of Mac OS X, see the document "Designing AirPort Extreme Networks," located at www.apple.com/airport.

What Is AirPort Client Monitor?

A wireless LAN (WLAN) that is not designed and installed properly can experience performance issues ranging from areas with no signal (or "dead spots") and low transmission rates to connection problems and increased network latency. AirPort Client Monitor gives network administrators the tools to plan for the installation of the network, as well as monitor connection information, such as transmission rates and the signal quality between the base station and the wireless client. It is an excellent planning and survey tool that can be used in a site survey to help determine the best settings and locations for base station placement. For more information about using AirPort Client Monitor when doing a site survey, see Chapter 2, "Performing a Site Survey," on page 21.

Using AirPort Client Monitor, wireless clients can get data over a range of time, as well as save a snapshot of their network connection status as a PDF file.

What Is AirPort Management Utility?

AirPort Management Utility is a wireless network management utility that offers network administrators powerful setup, management, and monitoring tools for larger AirPort networks. AirPort Management Utility provides an easy way for wireless network administrators to get status from a single base station, a group of base stations, or all of the base stations on the network.

AirPort Management Utility is not designed to replace AirPort Admin Utility, but rather work in conjunction with it. Use AirPort Admin Utility to set up a "master" base station or base stations, and then save the base station configuration file. AirPort Management Utility uses the configuration file as a starting point to configure the other base stations on your network.

Using AirPort Management Utility, network administrators can create groups of base stations, which can be monitored, adjusted, or updated. For example, all of the base stations on a particular floor of a building, or all base stations using a particular channel can be grouped together for ease of management and organization.

AirPort Management Utility offers powerful tools for these network management tasks:

- Managing groups of base stations
- Updating multiple base station configurations
- Viewing summary information
- Logging base station events
- Base station client monitoring

AirPort Management Utility is designed to manage networks with a large number of AirPort Base Stations. If your network has only a few base stations, use AirPort Admin Utility to manage them. You can open a base station configuration in AirPort Admin Utility from AirPort Management Utility. Just select the base station and click the "Open in Admin Utility" icon in the toolbar.

Managing Multiple AirPort Base Stations

Use AirPort Management Utility to create groups of base stations and simplify management of the base stations on your network. For example, you could create a group for all of the base stations on the second floor of your building, or all of the base stations broadcasting on channel 6.

Viewing Summary Information

Quickly see the base station name, MAC address, IP address, and firmware version of a single base station, a group of base stations, or all the base stations on your network.

Updating Multiple Base Stations on Your Network

Upload a new configuration file to a group of base stations, or all of the base stations on your network. Change all of the settings, or change just one setting, such as the wireless security mode of the network. You can also upload new firmware to all of your base stations, or just a group of base stations.

Base Station Logging

AirPort Management Utility can log the activity of any base station on the network. The data can be used to determine the general status of the network and the amount of activity taking place on any given base station.

Base Station Client Monitoring

Monitor the signal strength and noise of wireless clients connected to a base station on the network. Client monitoring can help network administrators troubleshoot problems by knowing precisely which configuration settings may need to be adjusted.

Client computers must be connected to the base station being monitored. AirPort Management Utility displays all of the client computers connected to the base station, and returns basic information about each client.

What's Included in This Guide

Chapter 1: Using AirPort in a Large Network

Read this chapter to familiarize yourself with general concepts related to designing, setting up, and managing a large wireless network.

Chapter 2: Performing a Site Survey

Read this chapter for information and tips on performing a site survey of your campus to help place base stations in the most effective spots.

Chapter 3: Using AirPort Management Utility

This chapter provides step-by-step instructions for using AirPort Management Utility.

Chapter 4: Real World Scenarios

This chapter gives some examples of how you can use AirPort Management Utility to keep the base stations on your wireless network up to date.

Using AirPort in a Large Network 1

AirPort offers an easy and affordable way to provide wireless Internet access and networking anywhere in the classroom, home, or office. Now AirPort Management Utility and AirPort Client Monitor provide powerful tools for planning, setting up, fine-tuning, and managing larger, enterprise-class wireless networks.

Wireless networking is becoming as common as wired networking. Wireless local area network (WLAN) technology allows you to extend an existing wired network into areas where hardwiring may be expensive and difficult. Apple's AirPort technology has made wireless networking in the home and small office easy and cost effective. With the introduction of Apple's AirPort Client Monitor and AirPort Management Utility, designing, setting up, and managing an enterprise WLAN is just as simple.

One of the best things about wireless local area networks (WLANs) is that they are so easy to set up. But while it's true that eliminating network wiring reduces the time and cost of providing Internet and network access, you can't just install base stations, call it an enterprise, and start broadcasting. You need to develop a wireless plan for your 802.11g network, just as you developed a wiring plan for your Ethernet network.

And because wireless networks use an unlicensed radio spectrum that's available to anyone with a wireless computer, network security is also very important.

Once you've decided to install an enterprise-class wireless network, you need to answer some important questions to avoid unnecessary problems:

- What kind of Internet and network connections does your network have?
- How large an area are you hoping to cover wirelessly?
- How many users will be using the wireless network in the same room at the same time?
- Will the signal need to pass through walls or other radio obstacles?
- Are there sources of interference nearby, such as cordless phones or microwave ovens?
- How secure do you need your network to be?
- Will you be sharing other network resources, like video streaming servers or printers?

Use this guide to help you answer some of these questions. Careful planning, implementation, monitoring, and management ensures your network is safe, efficient, and always available.

This chapter provides an overview of the challenges of designing an enterprise-class WLAN:

- Considerations for 802.11 wireless networks
- Selecting the right security strategy
- Deciding where to place base stations
- Understanding and fine-tuning network performance

Considerations for 802.11 Wireless Networks

Setting up a wireless local area network can seem simple. Home users plug a base station into broadband link and start using it without further setup. But implementing a successful enterprise WLAN requires forethought and planning.

Some factors to take into consideration when planning for an enterprise-class wireless LAN include:

- The physical layout, coverage area, and obstacles within your facility
- The bandwidth required to support all of the users and applications
- The number of users accessing the wireless network
- Placement of the base stations
- Sources of interference
- Authentication and encryption methods
- The size of the wireless network and the need to scale it in the future
- Existing wired network design

These factors are discussed in the following sections.

Selecting the Right Security Strategy

The selection of authentication and data encryption methods for your WLAN depends on several factors. Your wireless security policy, the type of data you are trying to secure, and the complexity of the potential security solutions can all play a role in the type of authentication and data encryption you choose.

- Identify the security requirements for your wireless LAN. What are you trying to protect, and who should be given access to the wireless LAN?
- Identify and understand the benefits of each authentication and data encryption method, and the administrative resources required to set up and maintain each security feature.
- Test the security features you've chosen with your hardware and client software to make sure they fit your needs.

Note: This chapter highlights the different authentication and data encryption options available for securing wireless LANs, but does not go into great detail about each one. For more information on wireless security and how to select a wireless security scheme, see the document "Designing AirPort Extreme Networks," located at www.apple.com/airport.

Authentication Methods

AirPort security options are made up of *authentication* and *encryption* methods. Authentication is used to regulate access and control who can join the wireless network. Encryption protects the data that's transferred over the wireless network.

AirPort uses authentication and encryption to deliver a level of security comparable to traditional wired networks. Users can be required to enter a password to log in to the AirPort network. When transmitting data and passwords, the base station uses up to 128-bit encryption, through either Wi-Fi Protected Access™ (WPA) or Wired Equivalent Privacy (WEP), to scramble data and help keep it safe.

There is currently a range of authentication methods available for wireless networks, and each has its advantages and disadvantages. The stronger the authentication, the greater effort required to set up and maintain the security solution. The most common authentication methods for wireless LANs include:

- **No Authentication:** This means there is no password protection for the network. Any computer with a wireless adapter or card can join the network.
- **Access Control (MAC Address Filtering):** Every AirPort and wireless card has a unique MAC address, sometimes referred to as the AirPort ID. Support for MAC (media access control) address filtering lets administrators set up a list of MAC addresses and restrict access to the network to only those users whose MAC addresses are on the access control list.

- **Wired Equivalent Privacy (WEP):** Choose either 40-bit or 128-bit encryption to protect your network with a Wired Equivalent Privacy password.
- **Wi-Fi Protected Access (WPA) and 802.1X:** This version of AirPort supports WPA, the latest security standard for wireless networks. Using Mac OS X 10.3 and its 802.1X authentication capabilities, WPA security delivers more sophisticated data encryption than WEP, and also provides user authentication, which was virtually unavailable with WEP.
- **Third-party Virtual Private Network (VPN) authentication:** A VPN uses the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as Layer Two Tunneling Protocol (L2TP), or Internet Protocol Security (IPsec).

Some of these authentication methods can be combined to create stronger security solutions. Access control, for example, can be applied to any of the other authentication methods. Smaller wireless networks that do not need the complexity of a RADIUS server may choose WPA Personal combined with access control to control user access. For networks requiring stronger authentication, 802.1X with a secure EAP type (see below) may be the best choice. These can also be combined with access control for very high security.

There is a tradeoff between strong security and ease of setup and management. Using a strong authentication scheme with 802.1X, for example, requires the selection of an Extensible Authentication Protocol (EAP) technology. Depending on your security requirements, the EAP method you select may complicate your network setup, especially if you select EAP-TLS. The most common EAP types include:

- **EAP-TTLS (Tunneled Transport Layer Security)** is an extension of EAP-TLS (see below) that provides for certificate-based, mutual authentication of the client and network through an encrypted channel (or "tunnel"), as well as a means to derive dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires certificates only on the server.
- **PEAP (Protected Extensible Authentication Protocol)** provides a method to securely transport authentication data, including legacy password-based protocols, over 802.11 wireless networks. PEAP tunnels between PEAP clients and an authentication server. Like TTLS, PEAP authenticates wireless LAN clients using only server-side certificates, simplifying the setup and administration of a secure wireless network.

- **EAP-TLS (Transport Layer Security)** provides for certificate-based, mutual authentication of the client and the base station. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the base station. One drawback of EAP-TLS is that certificates must be managed on both the client and server. For a large WLAN installation, this could be a very cumbersome task.

There are other EAP types, such as LEAP and EAP-MD-5, but the EAP types listed above are used most commonly in AirPort and other wireless networks.

Use the following table to understand the levels of security and complexity of each authentication type.

802.1x EAP	TTLS	PEAP	TLS
Client-side certificate required	No	No	Yes
Server-side certificate required	Yes	Yes	Yes
WEP key management	Yes	Yes	Yes
Authentication attributes	Mutual	Mutual	Mutual
Difficulty	Moderate	Moderate	Very
Security	High	High	Highest

Data Encryption Methods

Once you have selected an authentication method for your WLAN, you need to select an encryption scheme to protect the data packets traveling over the wireless network. Some of these encryption schemes can only be used with specific authentication methods. And not all wireless network cards or computer operating systems support the latest and strongest encryption methods. If you plan to include computers using operating systems other than Mac OS X v10.3 or later, you may need to purchase third-party 802.1X client software if you select WPA as your standard.

Each authentication method can be combined with a data encryption method to help secure the wireless network.

For enterprise-class wireless security, the minimum security standard that should be considered is WPA Enterprise. WPA uses 802.1X to provide strong authentication and dynamically generates a unique encryption key for every user on the wireless network. Every time the user connects to the wireless LAN, a new, unique key is created and assigned to the user.

Many security choices can help secure the wireless network. As the need for security rises, the complexity of network setup and management also increases. When looking at the security features, review what your existing wireless clients support. Computers using AirPort support all of the authentication and encryption methods mentioned above. Make sure that computers using other wireless cards are fully compatible with the security provided by the AirPort Extreme Base Stations or WLAN switch you use on your network.

Deciding Where to Place the Base Stations

The next step in wireless network design is to determine how many base stations you'll need on your network, and where to place them for optimum network coverage, efficiency, performance, and security.

As radio waves travel through the air, the signal is scattered over a wider and wider area until it finally dissipates. Wireless client computers that are closest to the base station receive the strongest signal and can send data faster, while client computers that are further from the base station receive a weaker signal and operate at a slower speed. The relationship between distance and data rate is illustrated in *Figure 1,* where three base stations are used to create a WLAN covering one floor of a building.

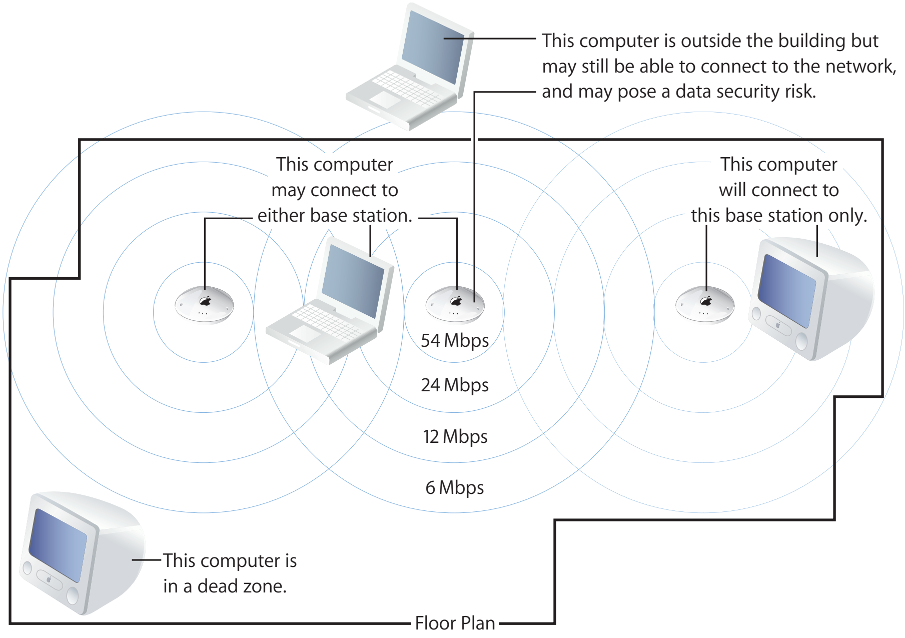

This computer is outside the building but may still be able to connect to the network, and may pose a data security risk.
This computer may connect to either base station.
This computer will connect to this base station only.
54 Mbps
24 Mbps
12 Mbps
6 Mbps
This computer is in a dead zone.
Floor Plan

Figure 1 Signal ranges in a network with multiple base stations

Wireless client computers connect to the base station that offers the strongest signal and highest data rate, unless they are configured not to. If signal quality degrades, the data rate drops automatically. When a wireless computer determines that conditions have changed and another base station offers a better signal, it tries to connect with the new base station. For example, in *Figure 1,* the computer on the right side will most likely associate with the base station on the right. The computer in the middle will roam between the base station in the middle and the base station on the left, depending on environmental conditions that affect signal strength, including obstacles and sources of interference.

Base stations should be positioned with some coverage overlap to avoid areas with no signal ("dead spots"). An ideal base station layout uses overlap to provide enough signal for all client computers under normal conditions. In *Figure 1,* 12 Mbps or better should be available to all computers located along the horizontal center of the floor. Computers located along the walls receive little or no signal. For example, the computer at the bottom-left of the figure is located in a dead spot. When placing base stations, try to make sure dead spots are located in corners and outside walls, or in hallways or stairwells where coverage isn't needed.

Why not install more base stations to provide higher throughput to all computers without any dead spots? There are several things to take into consideration before setting up more base stations in the same area.

- Locating more than one base station in the same spot is more expensive, but can support a high concentration of users in one location (in a classroom, for example), or in places where high bit-rate applications are needed (like streaming video). In *Figure 1,* for example, a high-throughput 54 Mbps "hot spot" is provided at the center of the floor by setting up a single 802.11g AirPort Extreme Base Station.
- If there are too many base stations set up too closely together, the signals will overlap. If base station coverage overlaps too much, computers located in the center of *Figure 1* will repeatedly roam. If the computer is a stationary, desktop computer, it may bounce between base stations. Roaming for stationary computers should be the exception, not the rule.
- When coverage overlaps, co-channel interference causes the signals to degrade, resulting in data loss and reduced data rates. Assigning channels with maximum separation can eliminate this interference. In *Figure 1,* for example, assigning each base station a channel that is separated by 4 channels from the next base station (channels 1, 6, and 11, for example) will eliminate co-channel interference. However, 802.11 transmissions still bleed a bit outside of the defined range for each channel, so some co-channel interference may still exist. If unacceptable interference persists, reposition adjacent base stations or reduce transmitter power.

- The computer outside the building in *Figure 1* is within the WLAN's "footprint." This illustrates a potential security risk created by radio signals that leak beyond the intended coverage areas. Unauthorized users in adjacent hallways, parking lots, or floors can take advantage of this leakage and attempt to connect to your network. Using access control and authentication security measures can help address this risk. You can also reduce the risk of leakage through careful placement of the base stations, and by adjusting the transmitter power of each base station.

Understanding and Fine-Tuning Network Performance

The illustration in the previous section shows the signal ranges of the base stations as perfect circles. In reality, coverage is not this uniform. Signal strength and data rates are affected by many factors.

Interference: Interference created by devices broadcasting in the 2.4 GHz band is common and can have a huge impact on wireless LAN performance. Since the 2.4 GHz is a shared spectrum, your network needs to take into consideration the interference created by cell phones, microwave ovens, cordless telephones, radios, satellite disks, lighting systems, some baby monitors, and some Bluetooth devices.

Obstacles: As radio waves move through the air, they are absorbed by solid objects in their path, including wood, drywall, water, and human bodies. Obstacles cause signal strength to be reduced, and result in lower data rates and unexpected dead spots. Relocating base stations can help. Placing base stations in the center of a large open space instead of next to a solid-core wall or under a wooden desk can help reduce signal degradation. Also, transmission power can be increased or external antennas can be used to better focus power output.

Multipath: As radio waves propagate, they bounce off reflective surfaces, causing copies of the same wave to arrive at the receiver at slightly different times. This phenomenon may cause the signal to be amplified, reduced, cancelled out, or corrupted. AirPort Extreme Base Stations compensate for this, but you may need to move base stations located next to metal and other smooth, flat surfaces.

Interference from other computers: Computers transmitting with high power very close to a base station may inhibit transmission by computers further away. This problem may be intermittent. The distant computer's performance may be fine when other computers are not transmitting, but their performance may get worse when "louder" computers are active. To overcome these issues, reduce the transmitter power output of base stations near a group of computers or increase the transmitter power output of base stations far away from the computers.

Hidden nodes: Two computers can be within a base station's coverage area but not within reach of each other. Because these computers will be communicating on the same channel, but are hidden from each other, they are considered "hidden nodes." Hidden nodes are more likely to cause collisions, resulting in data loss, retransmission, and loss of throughput.

For many of these issues, relocating base stations and stationary computers can be helpful. You can further fine-tune your network by changing the channels the base stations use, or adjusting the base station transmitter power.

Channel Assignment

In most WLANs, you can set up base stations to communicate over a fixed channel that you select. Adjacent base stations should be at least four channels apart for the best signal management. For example, if base station A is set to channel 1, base station B should be set to channel 6 or higher.

Although the only way to eliminate co-channel interference is to separate adjacent base stations by at least 4 channels (channels 1, 6, and 11), in networks where there are more base stations than available channels, separating base stations by 3 channels (1, 4, 7, and 11) and reducing transmitter power to under 5 milliwatts can minimize co-channel interference.

AirPort Extreme Base Stations can automatically select any unused channel and then remain with that channel over time, but setting fixed channels according to a channel selection scheme helps ensure the best transmission and reception.

You don't need to assign channels for client computers; clients automatically discover the channel the AirPort network is using.

Wireless client computers try to connect to any base station broadcasting a desired network name (sometime referred to as Service Set Identifier, or SSID). Client computers connected to the network roam across base stations as they move or respond to signal strength changes, changing channels as they roam. When separate base stations support different groups of client computers (using access control for example), clients locate the right base station by using the network name, not the channel.

Transmitter Power

You can adjust the transmitter power settings of AirPort Extreme Base Stations to optimize coverage. Transmitter power can be increased to overcome data loss, eliminate dead spots, and boost data rates, or decreased to reduce co-channel interference or leakage outside the desired coverage area. By lowering the transmitter power, you can confine the network to a single classroom, for example. Output power is measured in milliwatts (mW) and can be set in one milliwatt increments, from 1 mW to 32 mW.

Antennas

The antennas included in AirPort Extreme Base Stations are omni-directional Dipole antennas. Dipole coverage looks like a flattened hemisphere; power radiates outward horizontally and to a lesser degree out of the top or bottom of the antenna. For example, a base station on the second floor of a building provides the strongest signal to computers on the same floor, and a weaker signal to computers on floors above and below, depending on the base station's power output.

You can connect an external antenna to an AirPort Extreme Base Station to change the characteristics of the antenna's coverage. External antennas focus the signal in a particular way, depending on the type of antenna. Directional antennas focus the base station's power output in one horizontal or vertical direction.

External antennas are usually mounted on walls or ceilings. They produce hemispherical coverage 30 to 180 degrees wide, facing away from the antenna's mount point. Directional antennas improve WLAN performance without extending the radio coverage into unintended areas.

Determining Required Bandwidth

Another consideration in your wireless network design is the minimum acceptable bandwidth each wireless user should have. By default, wireless client computers connect to the base station with the best signal. If there are many wireless users concentrated in one area, a single base station may support the majority of these users, but the available bandwidth is limited because bandwidth is shared between all users connected to the base station. When one client transmits data, all others must wait before they can transmit.

When calculating minimum bandwidth for each wireless client, consider the distance from the base station as well as the necessary bandwidth. As clients move farther from the base station, their ability to use the available bandwidth will decrease.

For example, let's say you want to ensure a minimum of 500 Kbps of actual throughput for each wireless user, and you're using an AirPort Extreme Base Station with a maximum throughput of 24.4 Mbps.

Actual Maximum TCP Throughput:	24.4 Mbps
Desired Minimum TCP Throughput per User:	500 Kbps (.5 Mbps)

To find the number of users the base station can support at the desired throughput, divide the base station's maximum throughput by the desired throughput:

24.4 Mbps /.5 Mbps = 48.8 Users

The performance that each of the 48 users would experience also depends on the applications that are running over the wireless LAN. Large file transfers or applications that require a lot of bandwidth (such as streaming audio or video) will affect the performance for all users connected to the base station. Performance is also affected by environmental conditions, such as obstacles and sources of interference. For more information about sources of interference, see "Items That Can Cause Interference With AirPort" on page 57.

You can also limit the number of users that can connect to each base station, thus providing a level of service that is acceptable to your users. To provide additional coverage and capacity, install additional base stations in the same general area to help balance the number of users that need to be supported. Use the information in the previous sections to optimize the placement and settings for additional base stations.

Here's a commonly used formula to calculate the approximate bandwidth provided to each wireless user:

(Base Station's Maximum Data Rate / 2) / Maximum Users = Maximum Bandwidth per User

For example, if the base station supports a maximum data rate of 54 Mbps and it was set up to allow 25 users to connect to it, the maximum bandwidth per user would be:

(54 Mbps / 2) / 25 Users = 1.08 Mbps per User

Note: Actual bandwidth will vary, depending on the number of users on the network, the size of file transfers, and other environmental conditions.

Surveying the Network Location

To determine how many base stations are required and where to place each one, you should perform a site survey. The results of your site survey help you determine the coverage patterns, capacity, channel selection, and power requirements of each base station on the wireless network.

When performing a site survey, take the minimum acceptable bandwidth into consideration. As you walk around to determine the coverage pattern and the signal strength of the base station, also note the maximum distance from the base station before an unacceptable performance level is reached.

The following chapter explains how to perform a thorough site survey, and suggests how best to use the information you gather to create an optimum wireless network.

Performing a Site Survey

2

Once you're familiar with the basics of wireless security, considerations for base station placement, and minimum bandwidth requirements, the next step is to perform a thorough site survey.

Any design you've created on paper needs to be refined to reflect the physical characteristics of the planned network site. The purpose of a site survey is to measure and document actual wireless activity at your site in order to refine your network design and satisfy user density, bandwidth, application throughput, coverage, and security requirements.

Step 1: Use a Map of the Facility and Usage Requirements

Before you can start plotting proposed base station placement, you'll need an accurate map of the building and floor(s) where WLAN service is going to be set up. Blueprints with actual layout and measurements are ideal. When creating a map by hand, draw rooms to scale, and include architectural features like stairwells, elevators, and support columns. The geographic coordinates of the facility and these features can also be helpful.

Next, mark up the facility map to identify areas where WLAN users will be located, as well as public areas where coverage is undesirable. For intended coverage areas, it is best to start by identifying how many users will require WLAN access at the same time, and what throughput each will require (average and maximum).

If users require continual WLAN access while roaming from one spot to another within the facility, it is important to identify spaces where continuous coverage is needed. For example, in a K-12 school, students may need access on a per-room basis, while teachers and administrators need a continuous connection across the campus. In higher education, continuous connections may be desirable, but security may be much more of an issue. Network segments may need to be restricted. In a retail store, workers may need to accomplish tasks from any location. In a hospital, nurses and doctors may require access to patient charts from anywhere in a ward, but radio use may not be permitted from operating rooms or radiology labs. Understanding the purpose of the WLAN is instrumental to addressing coverage needs.

It is also helpful to identify the location of existing power sources and network equipment on your map. For example, where are wiring closets, LAN switches, and uninterruptible power supplies located? Are there existing 802.11 base stations that need to be integrated into the new WLAN? Are there known sources of interference in the 2.4 GHz band (such as cordless phones or microwave ovens) that the new WLAN must avoid disrupting? Plotting the location of these devices in advance can save time during the survey by helping you anticipate what you will find there.

Obtain network topology diagrams to understand where wireless base stations will fit within the existing network. Although these diagrams come into play during network design, not the site survey, they can be useful to determine where base stations will be expected to connect to the wired LAN, as well as the network naming conventions employed at this site for various buildings, floors, rooms, and groups. Network diagrams can also help to identify any need for wireless bridging (to connect separate buildings, for example), in which case the site survey must include an analysis of possible locations for outdoor antenna placement.

Step 2: Assemble a Survey Kit

During an indoor site survey, place base stations in locations throughout the facility, plotting data rate boundaries (that is, the range of the base station signal at specific data rates), dead spots, and the impact of adjusting power output. To accomplish these tasks, you may need the following equipment and tools.

Base station: Use a dual-band base station with removable antenna and variable power settings to conduct site surveys. Consider bringing the base station you propose using at this site, like an AirPort Extreme Base Station and an external antenna.

Client computer: You will need at least one test computer with an AirPort Card or other wireless network adapter that is compatible with AirPort Client Monitor.

AirPort Client Monitor: Use AirPort Client Monitor to monitor and display the current data rate, channel, signal strength, and noise of the signal generated by the base station. It provides a foundation to loosely plot data rate boundaries and sample background noise. For small, informal site surveys, this may be sufficient.

External antenna: Using an external antenna during a site survey makes it easier to position the base station on walls or in the air spaces above suspended ceilings.

Battery pack and power converter: It is possible to rely on local power sources during the site survey, but it may be more convenient to bring a battery pack and DC-to-AC power converter. This lets you relocate the base station without worrying about wall sockets and extension cords. Bring extra batteries and/or rechargers for the wireless computer.

Physical measurement tools: Bring tape measures, string, measuring wheels, and if possible, a handheld GPS to measure distance and location from Ethernet drops and power sources.

Recording tools: The map or floor plan of your facility, network topology charts, graph paper, pencils, and erasers.

Some site surveys may require more detailed information. In those cases you may need to use additional tools such as the following:

WLAN analyzer: To conduct more extensive surveys that require greater precision, use 802.11-capable WLAN analyzer software to record signal and noise measurements and create a list of other wireless devices (such as 2.4 GHz phones or microwave ovens) as well as other base stations and channels they are using. Some analyzers are combined with a GPS to record the latitude and longitude associated with measurements.

Note: Macintosh computers do not currently support WLAN analyzers. If you plan to use a WLAN analyzer in your survey, you will need to use a computer other than a Macintosh.

Spectrum analyzer: To understand and diagnose sources of interference in challenging radio environments, like hospitals, a portable radio spectrum analyzer can be helpful. A WLAN analyzer may tell you that noise exists; a spectrum analyzer can help you pin down the noise source by examining frequency distribution.

Discovery software: Use discovery software, like MacStumbler or KisMAC, to help detect wireless networks using your AirPort Card or AirPort Extreme Card. The software displays information about nearby 802.11b and 802.11g wireless base stations, and can be used to diagnose wireless network problems.

Note: Apple does not provide support for third-party software.

Step 3: Conduct the Survey

Make sure you have access to wiring closets, adjacent floors, and other locations that may require special permissions.

Following steps 1 and 2 completely will better prepare you for the site survey.

Starting with your map, tour the entire facility, and review and plot the location of physical items you need to take into consideration, including wireless closets, power sources, elevators, and support columns. Look for radio obstacles like metal blinds, fire doors, solid-core walls, and radiographic equipment. Your goal is to verify that your facility map is correct, and to add any objects to it that you discover during the survey, so that you have a complete and accurate picture of the site.

During the survey, carry your portable computer with the discovery software set to channel-scanning mode (hopping across all channels, recording any existing base stations or client computer discovered). Identify all sources of potential interference, including the names of existing wireless networks, their channels, MAC addresses, signal strength, and location.

When you discover a signal, watch the signal strength and try to walk in the direction of the transmitter until you find it—be prepared to look upstairs, downstairs, and outside.

Using AirPort Client Monitor

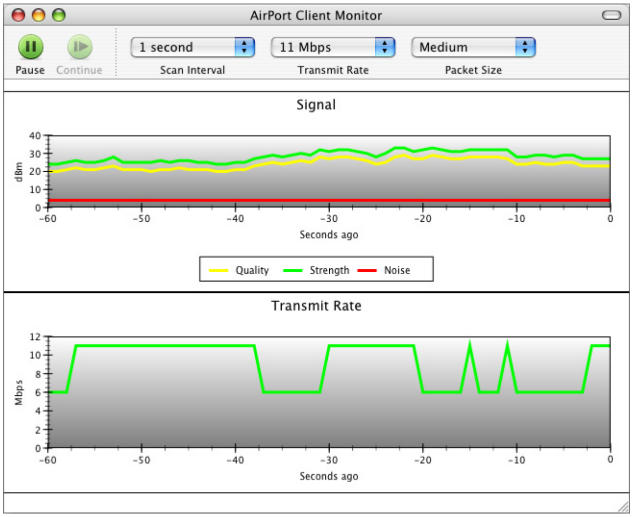
The next step is to plot the location of your base station to provide the desired coverage (data rate boundaries, signal strength, noise level, signal-to-noise ratio, dead spots). Place the base station in a proposed location, such as the center of a large open space or on the wall at the end of a long, narrow room. Then use AirPort Client Monitor on an AirPort-equipped computer to chart a coverage area around the base station that provides the bandwidth and signal quality you determined users will need. See "Determining Required Bandwidth" on page 18.

To use AirPort Client Monitor:

Make sure you are connected to the base station whose connection information you want to monitor.

1. Open AirPort Client Monitor.
2. Choose a time increment from the Scan Interval pop-up menu. This setting determines how frequently AirPort Client Monitor checks the signal. You may want to choose a smaller increment, such as 1 or 5 seconds, to get a more accurate reading.
3. Choose a speed from the Transmit Rate pop-up menu. This transmit rate is the required bandwidth you determined in the previous chapter.
4. Choose a size from the Packet Size pop-up menu. Choose Small, Medium or Large, depending on the usage patterns of clients on the network. For example, if users will be transferring large amounts of data across the network, choose Large.
5. Starting at the base station, move slowly away from the base station until the bandwidth drops out of the range you determined, and mark the location on your facility map. Record the signal quality, noise, and data rate at regular intervals. Also record locations where data rate drops; these are your data rate boundaries. Repeat this in all directions until you cover the entire facility and all proposed base station locations.

During this process, adjust the transmitter power of the base station to increase or decrease its range. This may help the signal reach areas that are not covered, or help avoid interference between base stations.


AirPort Client Monitor

Scan Interval: 1 second
Transmit Rate: 11 Mbps
Packet Size: Medium

During this process, make a note of dead spots and check your map to make sure you have examined coverage in both areas where coverage is needed, and areas where you don't want the signal to extend. Check outside the room or facility. It can also be helpful to sample application throughput between the wireless computer and the base station. If it becomes clear that throughput or coverage requirements are not met by the initial base station placement, move the base station or adjust the power output. This process may be time-consuming, but a thorough survey that examines several alternatives is often necessary to optimize the WLAN's design.

Step 4: Document the Results

The finished site survey usually includes the facility map, marked up to show proposed base station locations, data rate boundaries, signal, noise, signal-to-noise ratio, application throughput, dead spots, sources of interference, and problem areas where security risk exists or performance requirements are not fully satisfied.

As you complete your WLAN design, you should also add the recommended channel assignments, multicast rates, and power settings for each base station to the map.

Figure 2 illustrates the proposed placement of base stations in a wing of a school, based on the bandwidth requirements of the wireless computers connected to the base stations.

The circles indicate the range of the base stations. The darker, inner circle represents the area of maximum base station throughput, and the outer circle represents the area of minimum acceptable throughput.

The size of the circles is determined by the transmitter power settings of the base stations.

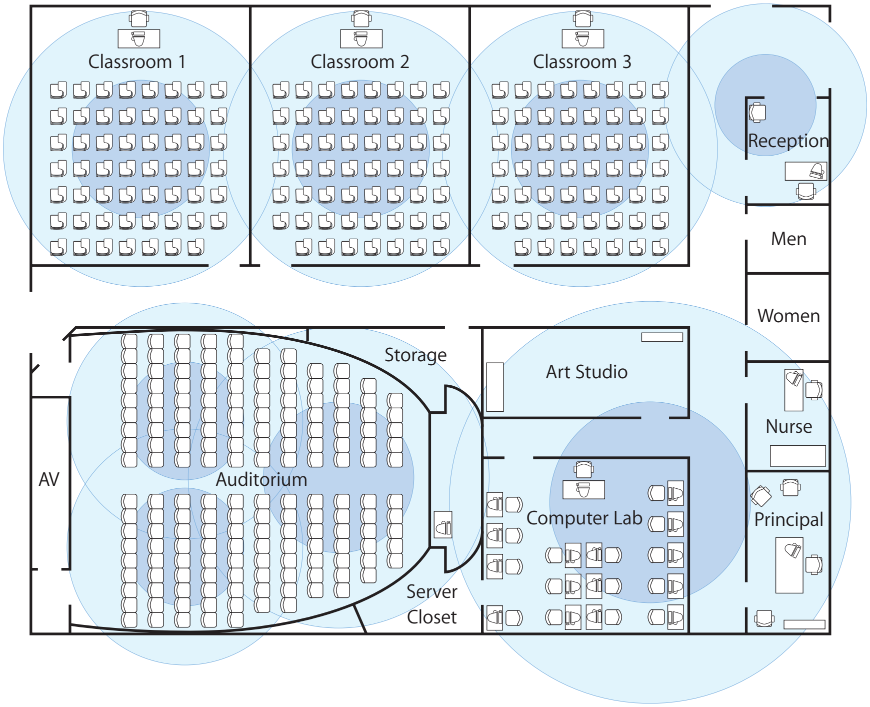


Figure 2 Site survey map

If this were an actual site survey, *Figure 2* might include actual data, including the channel assignment, transmitter power, and multicast rate of each base station.

It is important to note that the ranges of the base stations in *Figure 2* are represented as perfect circles. But results from your site survey will define imperfect shapes, determined by the transmission pattern of the base station, the bandwidth requirements of the client computers, the obstacles, and sources of interference described in the previous chapter.

The following table shows a chart that can be used to help keep track of base station channel selections and power settings. Remember to take adjacent floors into consideration, since radio signals can cross floors as well as walls.

	Location 1	Location 2	Location 3	Location 4	Location 5
Ground Floor	• Channel 1 • Power 20 mW • Base station 1-1	• Channel 6 • Power 20 mW • Base station 1-2	• Channel 11 • Power 20 mW • Base station 1-3	• Channel 1 • Power 20 mW • Base station 1-4	• Channel 6 • Power 10 mW • Base station 1-5
Second Floor	• Channel 11 • Power 20 mW • Base station 2-1	• Channel 1 • Power 20 mW • Base station 2-2	• Channel 6 • Power 20 mW • Base station 2-3	• Channel 11 • Power 20 mW • Base station 2-4	• Channel 1 • Power 10 mW • Base station 2-5

After you install the base stations, the site survey should be repeated again to verify and fine-tune results. In most WLANs, a less extensive site survey should be repeated at regular intervals to identify new (unknown or unauthorized) base stations and coverage changes resulting from reorganization, construction, or other changes to the facility.

The next section of this book describes setting up and using AirPort Management Utility. Use AirPort Management Utility to change configuration settings on one base station, or a group of base stations.

Using AirPort Management Utility

3

This chapter provides overview information and instructions for using AirPort Management Utility.

After completing your site survey, setting up your base stations, and fine-tuning the placement of the base stations, you need to be able to manage, monitor, and change the configuration settings on the base stations on your network.

AirPort Management Utility is an application that allows WLAN administrators to manage multiple base stations from a single location. Using AirPort Management Utility, you can add a new base station configuration, change an existing configuration, upload firmware to one, some, or all of the base stations, and monitor various properties of the base stations. AirPort Management Utility can manage more than a hundred base stations, although your network may be smaller.

AirPort Management Utility doesn't replace AirPort Admin Utility, but works in conjunction with it. Use AirPort Admin Utility to set up a "master" base station or base stations, and then save the base station configuration file. AirPort Management Utility uses the configuration file as a starting point to configure the other base stations on your network.

To open a base station's configuration in AirPort Admin Utility from AirPort Management Utility, select the base station and click the "Open in Admin Utility" icon in the toolbar.

After using AirPort Management Utility to organize and fine-tune your base stations and their settings, you can save the settings for the whole network as an AirPort Management Configuration File. You may want to have different files for different uses of the same network. For example, you can set up your network with base station settings specific to a group of students that use the network on Tuesdays, and then save a different file with base station settings specific to students using the network on a different day.

In this chapter you will learn about:

- Organizing the base stations on your network into groups
- Reading summary information about base stations
- Importing base station configuration files
- Viewing and changing configuration settings for base stations
- Updating the firmware of the base stations
- Logging base station messages
- Monitoring wireless client activity

Organizing Your Base Stations Into Groups

When you first open AirPort Management Utility, there are two groups in the Groups list: Configuration Files and Rendezvous.

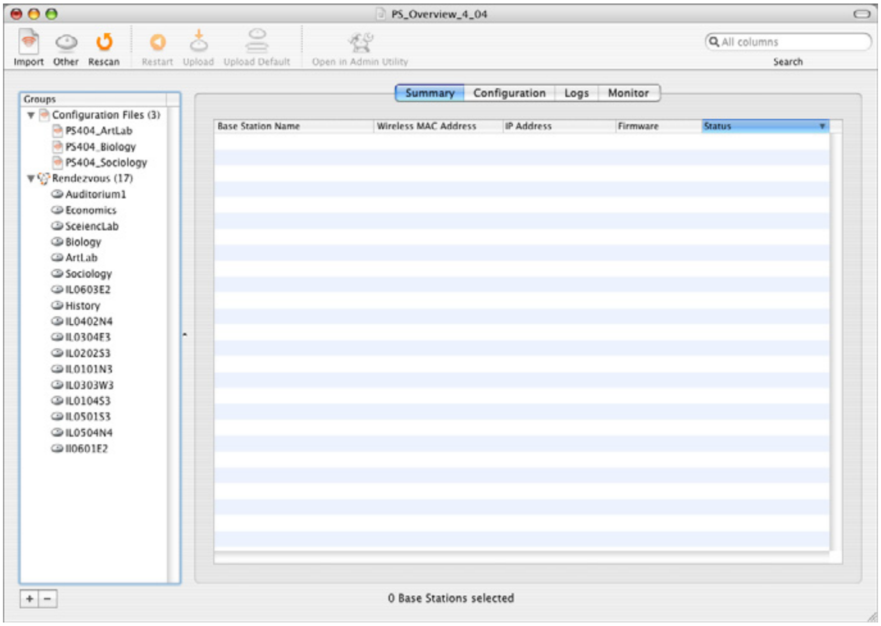
The first group contains configuration files created and saved using AirPort Admin Utility. You can import files into the list, then use the list to quickly access common configurations. For example, you could have a configuration file that turns on WPA, sets the base station to channel 7, or enables local access control. More commonly, you'll use a configuration in the list to serve as the standard configuration for new base stations.

The second default group is a list of base stations discovered using Rendezvous, Apple's network protocol that automatically discovers network resources on the local network. This group is a dynamic list that shows base stations on the local subnet only when they are available. The Rendezvous group displays information about each base station, such as the base station name (or SSID), its WAN port MAC address, its IP address, and the base station firmware version. This information helps you identify the base stations on your network.

When you open AirPort Management Utility, AirPort base stations on your local network are discovered automatically.

To add a base station that is not on your local network or subnet, click Other in the toolbar, and enter the IP address and password for the base station. AirPort Management Utility creates a new group in the Groups list, and adds the base station to the group.

Note: This version of AirPort Management Utility isn't compatible with the original, Graphite base station.



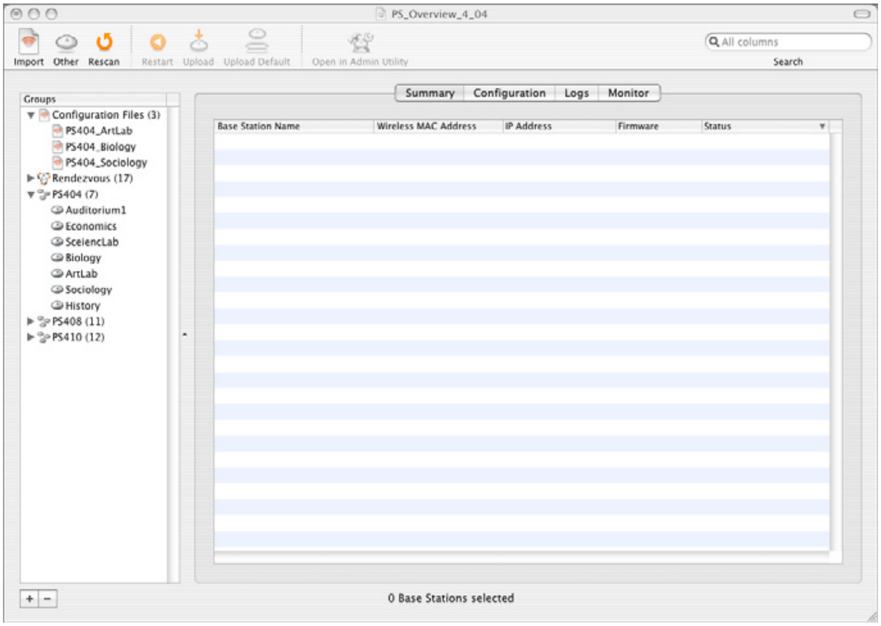
0 Base Stations selected

You can create your own groups of base stations to make it easier to manage multiple base stations at once.

To create a new group:

1. Click the Add (+) button below the Groups list.
2. Type a name for the new base station group.
3. Add base stations to the group by dragging them from the Rendezvous group to the new group.

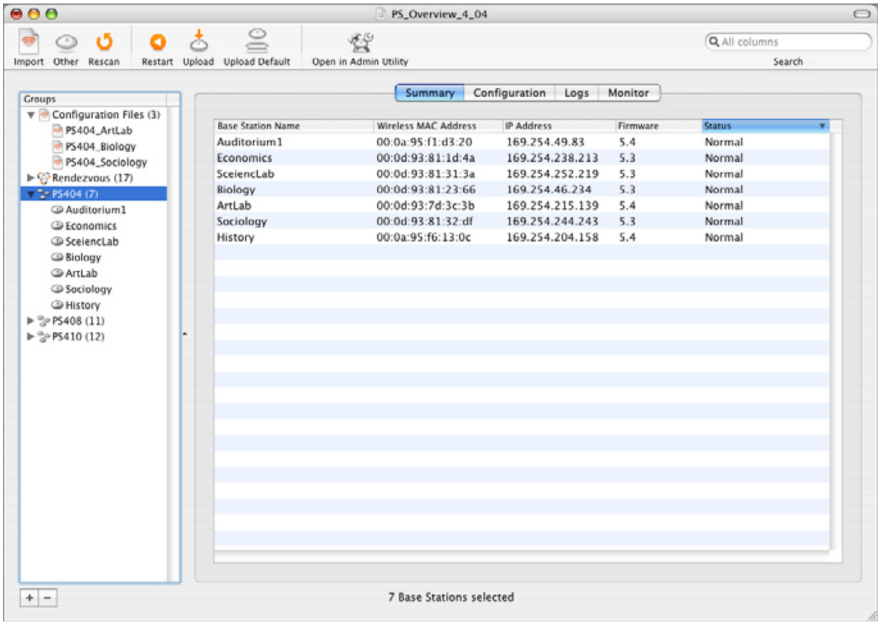
   You can add the same base station to multiple groups. For example, you could create a group called First Floor, and add all of the base stations on the first floor of your building to that group. You could also create a group called Channel 6, and include all of the base stations that use channel 6. If a base station on the first floor of your building also uses channel 6, you can include the base station in both groups.



0 Base Stations selected

Reading Summary Information

The Summary pane is the quickest way to review important information about each selected base station or group of base stations. It gives the most commonly needed information, such as the base station name, MAC address, IP address, and firmware version of each base station. To show summary information, select a base station or a group of base stations in the Groups list, and click Summary. If a group of base stations is selected, all of the base stations' summary information is displayed.



Base Station Name	Wireless MAC Address	IP Address	Firmware	Status
Auditorium1	00:0a:95:f1:d3:20	169.254.49.83	5.4	Normal
Economics	00:0d:93:81:1d:4a	169.254.238.213	5.3	Normal
SceiencLab	00:0d:93:81:31:3a	169.254.252.219	5.3	Normal
Biology	00:0d:93:81:23:66	169.254.46.234	5.3	Normal
ArtLab	00:0d:93:7d:3c:3b	169.254.215.139	5.4	Normal
Sociology	00:0d:93:81:32:df	169.254.244.243	5.3	Normal
History	00:0a:95:f6:13:0c	169.254.204.158	5.4	Normal

7 Base Stations selected

You can reorder and resize the columns in the Summary pane, and sort the list by selecting the name of a column, such as Firmware.

Importing a Base Station Configuration File

When you select a base station in a group, its configuration is displayed in the Configuration pane. The Configuration pane has three columns:

- **Name:** The name of the base station setting.
- **Current Setting:** The current value for the setting.
- **New Setting:** The new value you want to apply to the base station. Select the checkbox next to the new value to make it active.

Base station configuration files are created in AirPort Admin Utility, and contain all of the values for the different base station settings. After you have created the base station configuration file in AirPort Admin Utility, choose File > Save As and give the configuration file a name.

You can import base station configuration files into AirPort Management Utility, then apply them to any base station on your network. To import a base station configuration, you must have created and saved the configuration in AirPort Admin Utility.

To import a base station configuration:

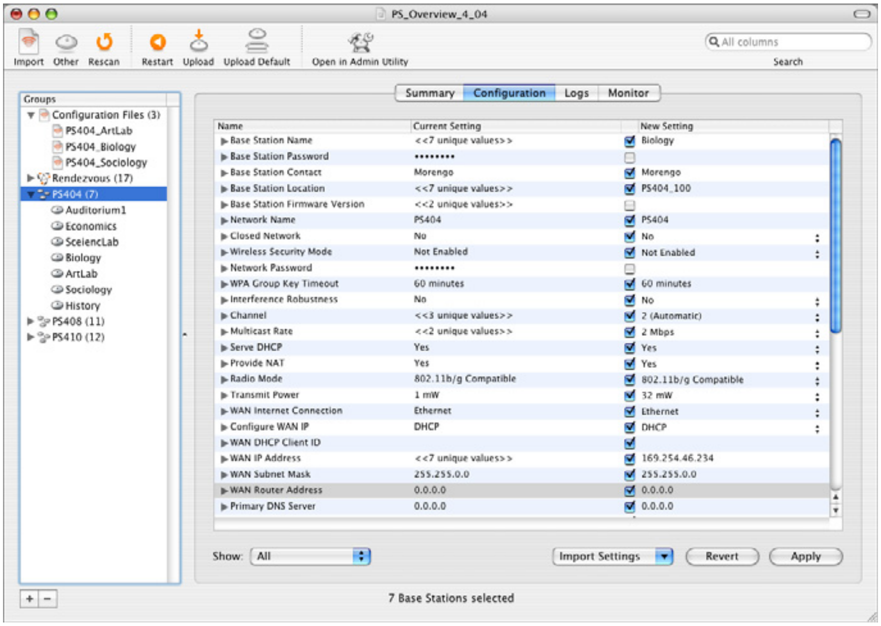
- Click Import in the toolbar, and select the configuration file you want to apply to the base station.

  Configuration files that you import into AirPort Management Utility are stored in the Configuration Files group in the Groups list.

To apply an imported configuration to a base station or group of base stations:

1. Select the base station or group of base stations in the Groups list.
2. Choose the configuration file from the Import Settings pop-up menu at the bottom of the Configuration pane.
3. Click Apply to send the new settings to the base station.

   You may need to enter the password for the base station before you can apply the new settings.



Name	Current Setting		New Setting
▶ Base Station Name	<<7 unique values>>	☑	Biology
▶ Base Station Password	••••••••	□	
▶ Base Station Contact	Morengo	☑	Morengo
▶ Base Station Location	<<7 unique values>>	☑	PS404_100
▶ Base Station Firmware Version	<<2 unique values>>	□	
▶ Network Name	PS404	☑	PS404
▶ Closed Network	No	☑	No
▶ Wireless Security Mode	Not Enabled	☑	Not Enabled
▶ Network Password	••••••••	□	
▶ WPA Group Key Timeout	60 minutes	☑	60 minutes
▶ Interference Robustness	No	☑	No
▶ Channel	<<3 unique values>>	☑	2 (Automatic)
▶ Multicast Rate	<<2 unique values>>	☑	2 Mbps
▶ Serve DHCP	Yes	☑	Yes
▶ Provide NAT	Yes	☑	Yes
▶ Radio Mode	802.11b/g Compatible	☑	802.11b/g Compatible
▶ Transmit Power	1 mW	☑	32 mW
▶ WAN Internet Connection	Ethernet	☑	Ethernet
▶ Configure WAN IP	DHCP	☑	DHCP
▶ WAN DHCP Client ID		☑	
▶ WAN IP Address	<<7 unique values>>	☑	169.254.46.234
▶ WAN Subnet Mask	255.255.0.0	☑	255.255.0.0
▶ WAN Router Address	0.0.0.0	☑	0.0.0.0
▶ Primary DNS Server	0.0.0.0	☑	0.0.0.0

Show: All

7 Base Stations selected

Viewing and Changing Configuration Settings

The Configuration pane allows you to see and modify base station settings. You can modify most of the settings with AirPort Management Utility, but some settings are read-only, such as distributing IP addresses using DHCP, or providing network address translation (NAT). To change settings that are read-only, use AirPort Admin Utility, save the configuration, and import it into AirPort Management Utility.

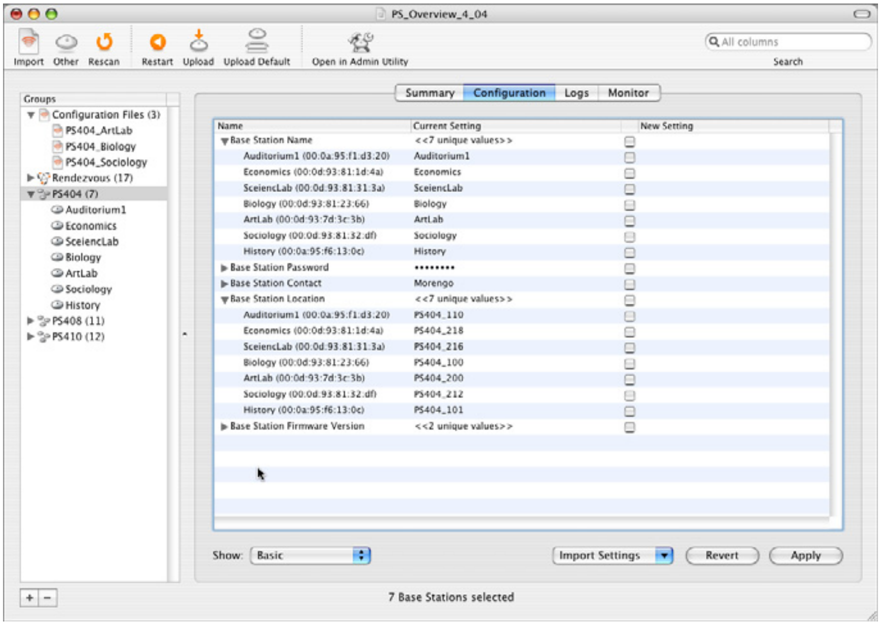
To view the settings of a base station or a group of base stations, select the base station or the group in the Groups list. The settings for that base station or that group are displayed in the Configuration pane. If you selected a single base station, only its settings are displayed. If you selected a group of base stations, there is a disclosure triangle next to the name of each setting. Click the triangle to view the settings for each base station in the group.

The list of settings is long, and includes most of the base station settings. Use the Show pop-up menu to see groups of related settings, instead of all settings at once.

The groups of settings are:

- **All:** Includes the entire list of settings.
- **Basic:** Includes only the base station name, password, and contact information.
- **Wireless:** Includes settings for the wireless network created by this base station, such as network name and password.
- **Radio:** Includes the channel, mode, and other information about the radio.
- **WAN:** Provides information about the WAN interface, such as its IP address, subnet mask address, and DNS server address.
- **Radius:** Displays RADIUS server information, such as the server's IP address and server type.
- **Misc.:** Contains settings such as local access control.

Choosing one of the groups of settings in the Show pop-up menu shows only the information for the list of settings in that group. Use the Configuration pane of AirPort Management Utility to change the settings of a base station or a group of base stations.



Name	Current Setting		New Setting
▼Base Station Name	<<7 unique values>>	□	
Auditorium1 (00:0a:95:f1:d3:20)	Auditorium1	□	
Economics (00:0d:93:81:1d:4a)	Economics	□	
SceiencLab (00:0d:93:81:31:3a)	SceiencLab	□	
Biology (00:0d:93:81:23:66)	Biology	□	
ArtLab (00:0d:93:7d:3c:3b)	ArtLab	□	
Sociology (00:0d:93:81:32:df)	Sociology	□	
History (00:0a:95:f6:13:0c)	History	□	
▶Base Station Password	••••••••	□	
▶Base Station Contact	Morengo	□	
▼Base Station Location	<<7 unique values>>	□	
Auditorium1 (00:0a:95:f1:d3:20)	PS404_110	□	
Economics (00:0d:93:81:1d:4a)	PS404_218	□	
SceiencLab (00:0d:93:81:31:3a)	PS404_216	□	
Biology (00:0d:93:81:23:66)	PS404_100	□	
ArtLab (00:0d:93:7d:3c:3b)	PS404_200	□	
Sociology (00:0d:93:81:32:df)	PS404_212	□	
History (00:0a:95:f6:13:0c)	PS404_101	□	
▶Base Station Firmware Version	<<2 unique values>>	□	

To change the settings for a base station or group of base stations:

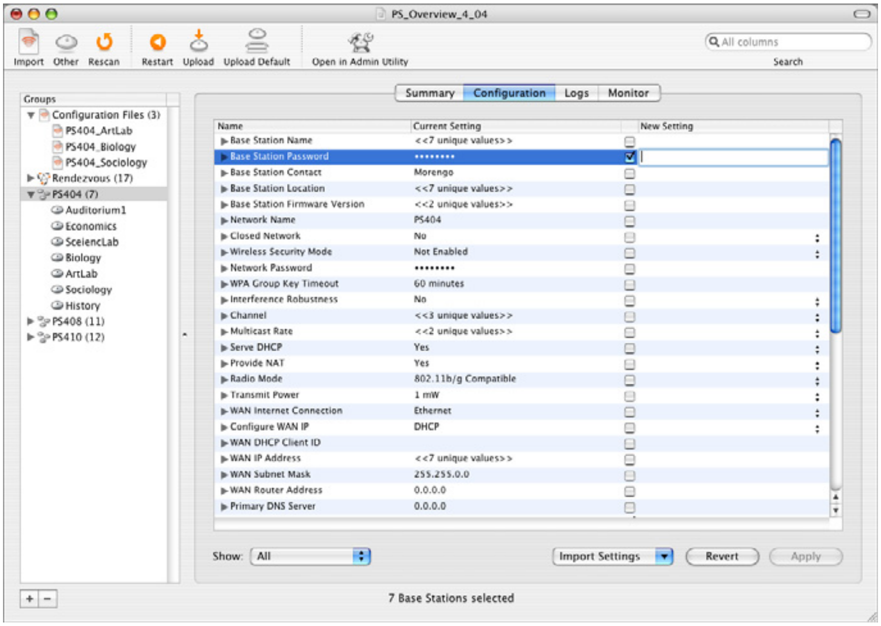
1 Select the base station or the group of base stations in the Groups list. The current settings for the base station or the group are displayed in the Configuration pane.

2 Select the checkbox next to the setting you want to change.

3 Double-click the setting field in the New Setting column of the Configuration pane, and enter a value for the new setting. If there are standard values for the setting (Wireless Security Mode, for example), click the double triangles on the right side of the New Setting column, and choose a setting from the list.

For Wireless Security Mode, the pop-up menu contains the wireless security options available for the base station: WPA Personal, WPA Enterprise, 128 bit WEP, 40 bit WEP, and Not Enabled.

4 Click Apply to send the new setting to the base station or base stations. You may be asked for the base station password(s).



Groups

- Configuration Files (3)
  - PS404_ArtLab
  - PS404_Biology
  - PS404_Sociology
- Rendezvous (17)
- PS404 (7)
  - Auditorium1
  - Economics
  - SceiencLab
  - Biology
  - ArtLab
  - Sociology
  - History
- PS408 (11)
- PS410 (12)

Name	Current Setting		New Setting
▶ Base Station Name	<<7 unique values>>	□	
▶ Base Station Password	••••••••	☑	
▶ Base Station Contact	Morengo	□	
▶ Base Station Location	<<7 unique values>>	□	
▶ Base Station Firmware Version	<<2 unique values>>	□	
▶ Network Name	PS404	□	
▶ Closed Network	No	□	⇕
▶ Wireless Security Mode	Not Enabled	□	⇕
▶ Network Password	••••••••	□	
▶ WPA Group Key Timeout	60 minutes	□	
▶ Interference Robustness	No	□	⇕
▶ Channel	<<3 unique values>>	□	⇕
▶ Multicast Rate	<<2 unique values>>	□	⇕
▶ Serve DHCP	Yes	□	⇕
▶ Provide NAT	Yes	□	⇕
▶ Radio Mode	802.11b/g Compatible	□	⇕
▶ Transmit Power	1 mW	□	⇕
▶ WAN Internet Connection	Ethernet	□	⇕
▶ Configure WAN IP	DHCP	□	⇕
▶ WAN DHCP Client ID		□	
▶ WAN IP Address	<<7 unique values>>	□	
▶ WAN Subnet Mask	255.255.0.0	□	
▶ WAN Router Address	0.0.0.0	□	
▶ Primary DNS Server	0.0.0.0	□	

Show: All

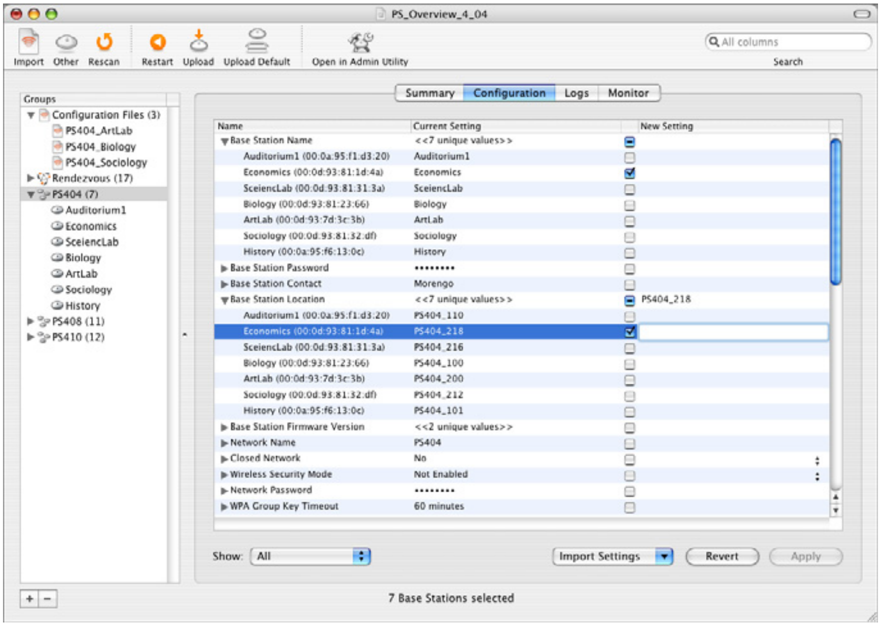
Import Settings

Revert

Apply

7 Base Stations selected

The procedure above changes settings for an entire group of base stations. But you can also send the new setting to individual base stations in the group. To change settings for individual base stations in a group, select the group of base stations in the Groups list, then click the disclosure triangle to the left of the setting name. The settings for the individual base stations in the group are displayed, and you can enter new values for each setting.



Name	Current Setting		New Setting
▼ Base Station Name	<<7 unique values>>	⊟	
Auditorium1 (00:0a:95:f1:d3:20)	Auditorium1	□	
Economics (00:0d:93:81:1d:4a)	Economics	☑	
SceiencLab (00:0d:93:81:31:3a)	SceiencLab	□	
Biology (00:0d:93:81:23:66)	Biology	□	
ArtLab (00:0d:93:7d:3c:3b)	ArtLab	□	
Sociology (00:0d:93:81:32:df)	Sociology	□	
History (00:0a:95:f6:13:0c)	History	□	
▶ Base Station Password	••••••••	□	
▶ Base Station Contact	Morengo	□	
▼ Base Station Location	<<7 unique values>>	⊟	PS404_218
Auditorium1 (00:0a:95:f1:d3:20)	PS404_110	□	
Economics (00:0d:93:81:1d:4a)	PS404_218	☑	
SceiencLab (00:0d:93:81:31:3a)	PS404_216	□	
Biology (00:0d:93:81:23:66)	PS404_100	□	
ArtLab (00:0d:93:7d:3c:3b)	PS404_200	□	
Sociology (00:0d:93:81:32:df)	PS404_212	□	
History (00:0a:95:f6:13:0c)	PS404_101	□	
▶ Base Station Firmware Version	<<2 unique values>>	□	
▶ Network Name	PS404	□	
▶ Closed Network	No	□	
▶ Wireless Security Mode	Not Enabled	□	
▶ Network Password	••••••••	□	
▶ WPA Group Key Timeout	60 minutes	□	

7 Base Stations selected

If all of the base stations in the group already have the same value for a setting, the value will be displayed without clicking the disclosure triangle. If the settings have different values, the number of unique values for the setting will be displayed.

If you enter new values in the New Setting column, and then decide you don't want to change the settings, click Revert to retain the old settings.

Updating the Base Station Firmware

You can use AirPort Management Utility to update the version of firmware on one base station, a group of base stations, or all of the base stations on your network. You need to have the firmware file on the computer where you are using AirPort Management Utility. Check the Apple website at www.apple.com/airport for the latest AirPort Extreme Base Station firmware.

To update the firmware on base stations on your network:

1. Open AirPort Management Utility.
2. Select the base station or group of base stations you want to update.
3. Click Upload in the toolbar and locate the firmware file.
4. Click Update. All of the base stations selected are reset with the new firmware file.

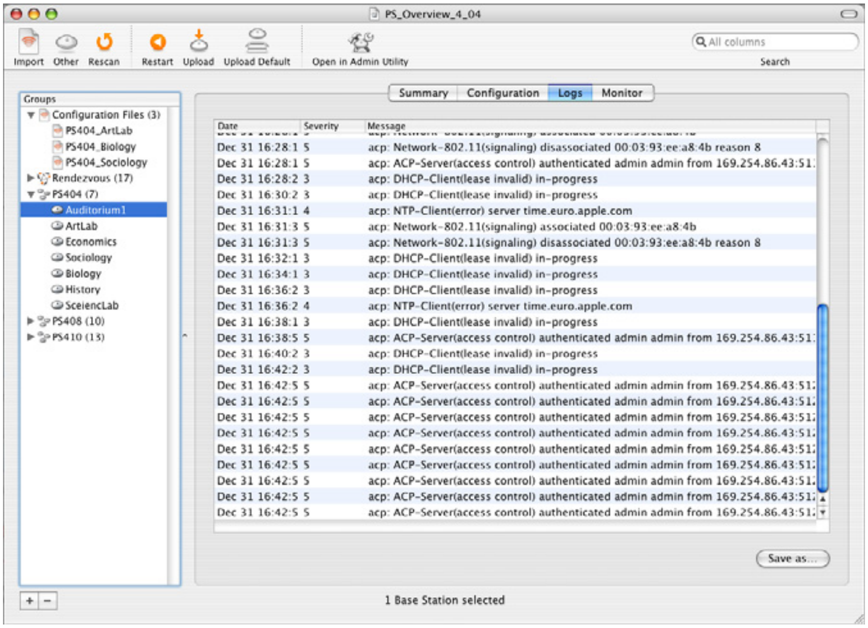
You can also click Upload Default in the toolbar to return the selected base stations to their original firmware.

Logging Base Station Messages

If you are using AirPort 3.4 or later, you can log status and error messages from AirPort Extreme Base Stations. If you have the BSD package installed on a computer using Mac OS X v10.3, you can view the log messages in the Console application (located in Applications/Utilities). You can also view the messages using AirPort Management Utility.

AirPort Management Utility shows log messages according to the way you set up the base station in AirPort Admin Utility. Even if the base station is configured to store messages on only one computer, you can use AirPort Management Utility to read the log messages of any base station on your network. However, AirPort Management Utility can only read log messages from one base station at a time.

When the Logs pane is visible, AirPort Management Utility queries the base station and retrieves the latest log messages. The date and time displayed in the log messages are determined by the Network Time Protocol (NTP) server you chose when you set up the base station in AirPort Admin Utility.



```
Date          Severity  Message
Dec 31 16:28:1 5        acp: Network-802.11(signaling) disassociated 00:03:93:ee:a8:4b reason 8
Dec 31 16:28:1 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:28:2 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:30:2 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:31:1 4        acp: NTP-Client(error) server time.euro.apple.com
Dec 31 16:31:3 5        acp: Network-802.11(signaling) associated 00:03:93:ee:a8:4b
Dec 31 16:31:3 5        acp: Network-802.11(signaling) disassociated 00:03:93:ee:a8:4b reason 8
Dec 31 16:32:1 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:34:1 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:36:2 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:36:2 4        acp: NTP-Client(error) server time.euro.apple.com
Dec 31 16:38:1 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:38:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:40:2 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:42:2 3        acp: DHCP-Client(lease invalid) in-progress
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
Dec 31 16:42:5 5        acp: ACP-Server(access control) authenticated admin admin from 169.254.86.43:51
```

There is no Start or Stop button. When the Logs pane is displayed, AirPort Management Utility is retrieving log messages.

To set up logging in AirPort Admin Utility:

1 Open AirPort Admin Utility, located in Applications/Utilities. Make sure you have joined the network of the base station you want to set up.

2 Select the base station and click Configure.

3 Click Base Station Options.

4 Select "Enable Base Station Logging to," and enter the IP address of the computer where you want to store the log, if you plan to view the log in Console.

If you plan to view the log in AirPort Management Utility, you can enter any IP address (such as 169.21.21.21) in the field. The log will be stored locally on the base station, not sent to a host computer.

5 Choose a level from the Logging Level pop-up menu.

6 Select Set Date & Time Automatically, and choose an NTP server from the pop-up menu. This will set the date and time of the log messages read in AirPort Management Utility.

To set up logging in AirPort Management Utility:

1 Open AirPort Management Utility.

2 Select the base station you set up in AirPort Admin Utility from the Groups list.

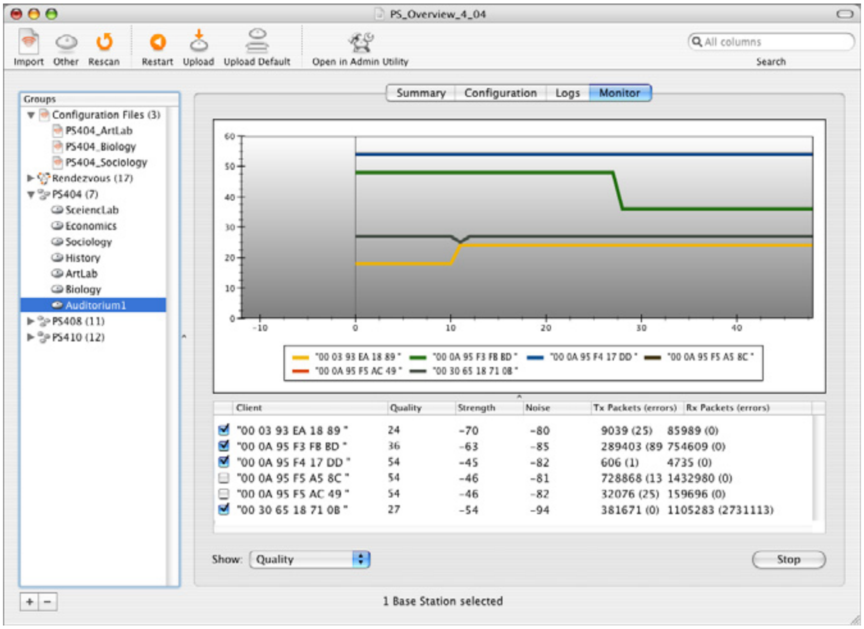
3 Click Logs.

The most recent log messages are displayed in the Logs pane. You can save the log messages as text files. This may be useful if you are troubleshooting a remote base station.

Monitoring Wireless Client Activity

You can use the Monitor pane in AirPort Management Utility to get information about the wireless clients connected to a base station on your network. When you open the Monitor pane, it uses Simple Network Management Protocol (SNMP) to query the base station for a number of values. (To use this feature, you must have the BSD package of Mac OS X installed.)

The query is sent every few seconds when the Monitor pane is visible. AirPort Management Utility displays signal quality, signal strength, or noise for each client computer connected to the base station. It also displays the number of packets sent and received, and an error count for each client computer.



	Client	Quality	Strength	Noise	Tx Packets (errors)	Rx Packets (errors)
☑	"00 03 93 EA 18 89 "	24	-70	-80	9039 (25)	85989 (0)
☑	"00 0A 95 F3 FB BD "	36	-63	-85	289403 (89	754609 (0)
☑	"00 0A 95 F4 17 DD "	54	-45	-82	606 (1)	4735 (0)
□	"00 0A 95 F5 A5 8C "	54	-46	-81	728868 (13	1432980 (0)
□	"00 0A 95 F5 AC 49 "	54	-46	-82	32076 (25)	159696 (0)
☑	"00 30 65 18 71 0B "	27	-54	-94	381671 (0)	1105283 (2731113)

Show: Quality

1 Base Station selected

You can use the columns in the Monitor pane to sort the information in the pane, and save the selected sort order as part of the AirPort Management Configuration File for that base station.

The Monitor pane displays only recent data and does not record any history beyond what is visible in the pane. You can monitor client computer activity on only one base station at a time.

The chart can be quite busy if there are dozens of client computers connected to the base station. Use the checkboxes in the table to control which client computers are being monitored.

To monitor the client computers connected to a base station:

1. Open AirPort Management Utility.
2. Select the base station you want to monitor in the Groups list.
3. Click Monitor, and then click Start.
4. If prompted, enter the base station password.
5. Choose Quality, Noise, or Signal from the Show pop-up menu.

What's Next?

Now that you understand the features of AirPort Management Utility, you can use it to:

- Manage the base stations on your wireless network
- Change or update configuration settings, such as base station contact information or transmitter power
- Monitor base station activity

The following chapter provides some examples of how AirPort Management Utility can make managing multiple base stations easy and efficient, and help keep your network up and running.

Real World Scenarios

4

This chapter provides some examples of how to use AirPort Management Utility to manage and update base station settings on your wireless network.

Use the examples in this chapter to help you understand how AirPort Management Utility can make changing common base station settings across your network fast and easy. Without AirPort Management Utility, making changes to multiple base stations requires locating each base station, connecting to it, and changing a setting. If your base stations are located in hard-to-reach places, this process can take a lot of time.

Using AirPort Management Utility to manage and monitor multiple base stations from a single location lets you optimize performance of the base stations, the network, and client computer connections without leaving your desk. Managing the base stations on your network from a single location also helps ensure the security of your network by restricting access to only those administrators using AirPort Management Utility.

Changing Contact Information

If your network is spread across multiple facilities, and base stations in each facility are managed by different people, you can change the contact information for base stations on the entire network quickly and easily. This is helpful if the person responsible for administering the base stations on the network changes, or that person's telephone number changes.

Using AirPort Management Utility, you can change the contact information in minutes, and save and distribute the new AirPort Management Configuration File to those who need to know whom to contact in case there's a problem with a base station in that facility.

To change the contact information for a base station or a group of base stations on your network:

1 Open AirPort Management Utility.

2 Select the group of base stations you want to change. If you haven't created a group, do the following:

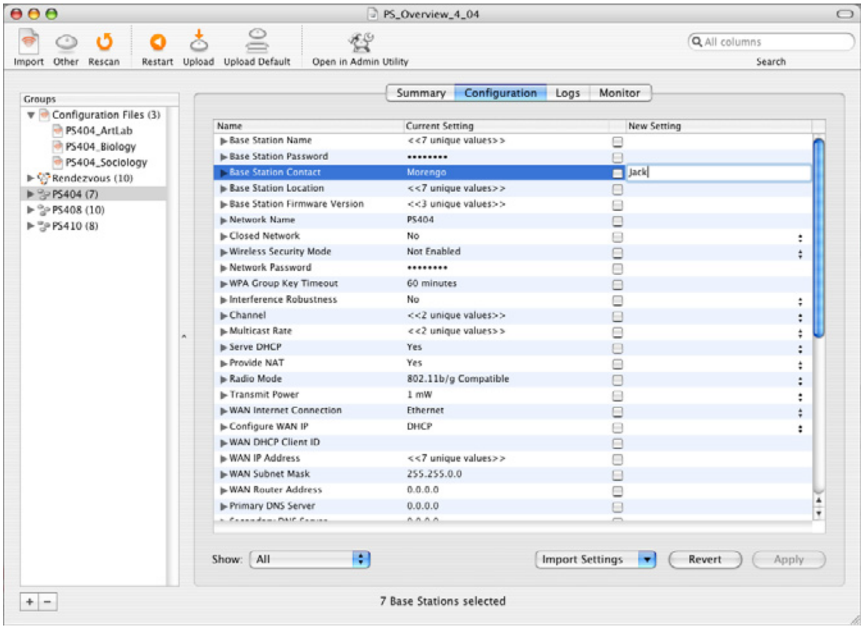
   a Click the Add (+) button at the bottom of the Groups list and give the group a name.

   b Select the base stations you want to add to the group from the Rendezvous group, and drag them into the group you just created.

3 Click Configuration, and if prompted, enter the password for the group of base stations. If the passwords are different for base stations in the group, you will be prompted for a password for each base station.

4 Select the Base Station Contact checkbox in the New Setting column, double-click the new setting field, and enter the new value.

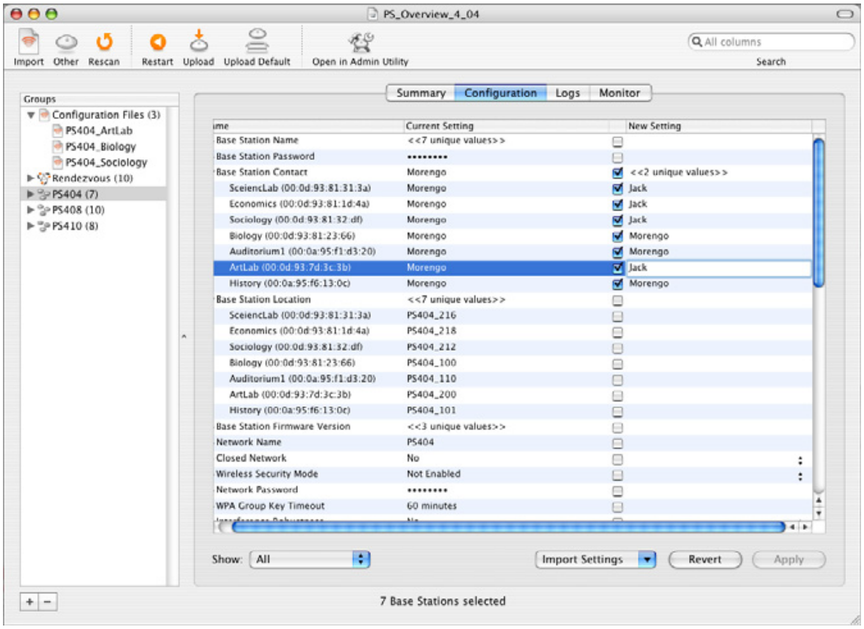
- If you are changing the contact information for the entire group of base stations, make sure the triangle to the left of Base Station Contact is not pointing down.



Name	Current Setting		New Setting
▶ Base Station Name	<<7 unique values>>	□	
▶ Base Station Password	••••••••	□	
▶ Base Station Contact	Morengo	□	Jack
▶ Base Station Location	<<7 unique values>>	□	
▶ Base Station Firmware Version	<<3 unique values>>	□	
▶ Network Name	PS404	□	
▶ Closed Network	No	□	
▶ Wireless Security Mode	Not Enabled	□	
▶ Network Password	••••••••	□	
▶ WPA Group Key Timeout	60 minutes	□	
▶ Interference Robustness	No	□	
▶ Channel	<<2 unique values>>	□	
▶ Multicast Rate	<<2 unique values>>	□	
▶ Serve DHCP	Yes	□	
▶ Provide NAT	Yes	□	
▶ Radio Mode	802.11b/g Compatible	□	
▶ Transmit Power	1 mW	□	
▶ WAN Internet Connection	Ethernet	□	
▶ Configure WAN IP	DHCP	□	
▶ WAN DHCP Client ID		□	
▶ WAN IP Address	<<7 unique values>>	□	
▶ WAN Subnet Mask	255.255.0.0	□	
▶ WAN Router Address	0.0.0.0	□	
▶ Primary DNS Server	0.0.0.0	□	
▶ Secondary DNS Server	0.0.0.0	□	

7 Base Stations selected

- If you don’t want to change the contact information for all of the base stations in the group, click the triangle to the left of Base Station Contact to reveal all of the base stations in the group. Select the checkboxes in the New Setting column for the base station or base stations you want to change, double-click the new setting field, and enter the new contact information.



ıme	Current Setting		New Setting
Base Station Name	<<7 unique values>>	☐	
Base Station Password	••••••••	☐	
Base Station Contact	Morengo	☑	<<2 unique values>>
SceiencLab (00:0d:93:81:31:3a)	Morengo	☑	Jack
Economics (00:0d:93:81:1d:4a)	Morengo	☑	Jack
Sociology (00:0d:93:81:32:df)	Morengo	☑	Jack
Biology (00:0d:93:81:23:66)	Morengo	☑	Morengo
Auditorium1 (00:0a:95:f1:d3:20)	Morengo	☑	Morengo
ArtLab (00:0d:93:7d:3c:3b)	Morengo	☑	Jack
History (00:0a:95:f6:13:0c)	Morengo	☑	Morengo
Base Station Location	<<7 unique values>>	☐	
SceiencLab (00:0d:93:81:31:3a)	PS404_216	☐	
Economics (00:0d:93:81:1d:4a)	PS404_218	☐	
Sociology (00:0d:93:81:32:df)	PS404_212	☐	
Biology (00:0d:93:81:23:66)	PS404_100	☐	
Auditorium1 (00:0a:95:f1:d3:20)	PS404_110	☐	
ArtLab (00:0d:93:7d:3c:3b)	PS404_200	☐	
History (00:0a:95:f6:13:0c)	PS404_101	☐	
Base Station Firmware Version	<<3 unique values>>	☐	
Network Name	PS404	☐	
Closed Network	No	☐	
Wireless Security Mode	Not Enabled	☐	
Network Password	••••••••	☐	
WPA Group Key Timeout	60 minutes	☐	

7 Base Stations selected

5 Click Apply to update the base stations with the new contact information.

Changing Bandwidth Allocation

If a department in your school starts a new project that requires students using the wireless network in a specific area to have a faster connection to the network, you can change the multicast rate of the base stations in that area.

Making minor adjustments to the multicast rate can help ensure everyone accessing the network has the speed and bandwidth they require to share their project files.

To change the multicast rate for a base station or a group of base stations on your network:

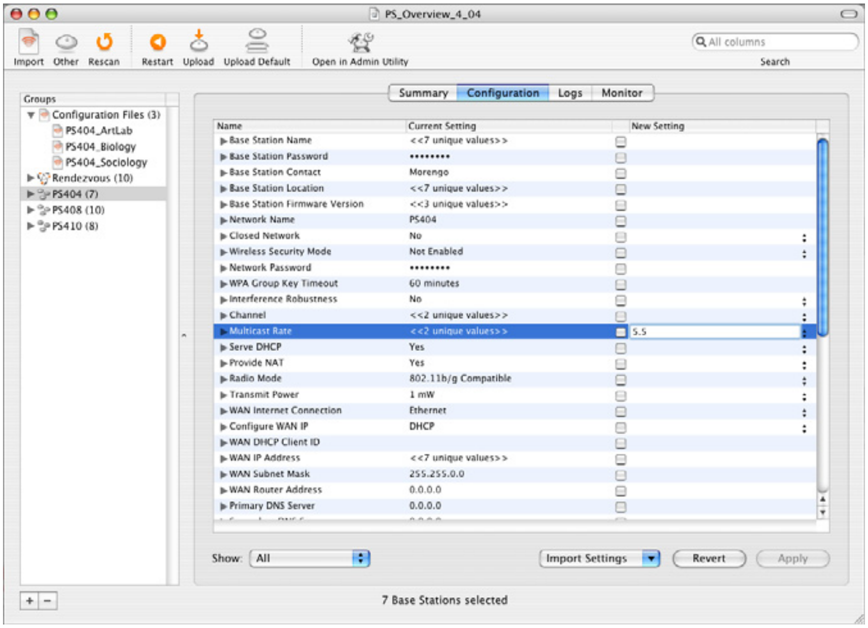
1 Open AirPort Management Utility.

2 Select the group of base stations you want to change.

3 Click Configuration, and if prompted, enter the password for the group of base stations. If the passwords for the base stations in the group are different, you will be prompted for a password for each base station.

4 Select the Multicast Rate checkbox in the New Setting column, double-click the new setting field, and enter the new value.

- If you are changing the value for the entire group of base stations, make sure the triangle to the left of Multicast Rate is not pointing down.



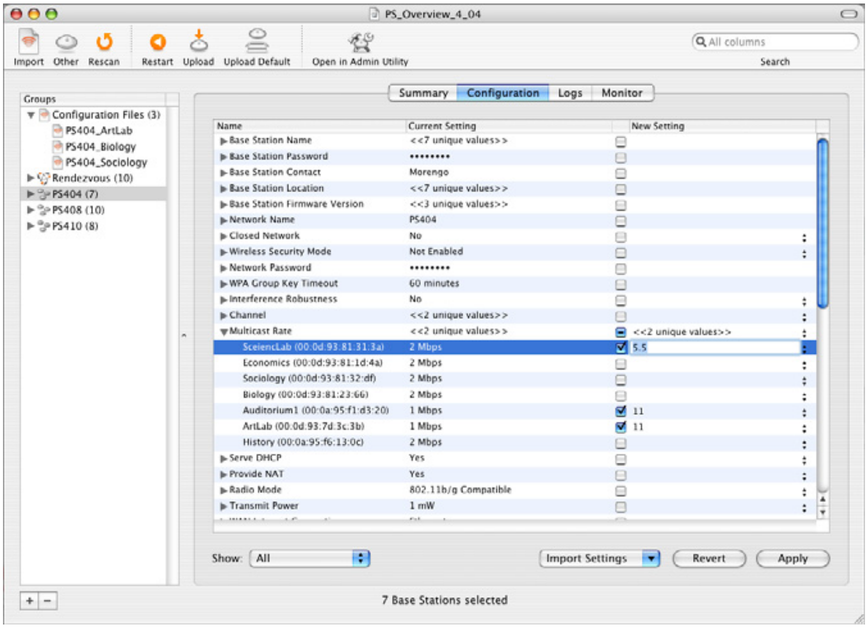
Name	Current Setting		New Setting
▶ Base Station Name	<<7 unique values>>	□	
▶ Base Station Password	••••••••	□	
▶ Base Station Contact	Morengo	□	
▶ Base Station Location	<<7 unique values>>	□	
▶ Base Station Firmware Version	<<3 unique values>>	□	
▶ Network Name	PS404	□	
▶ Closed Network	No	□	
▶ Wireless Security Mode	Not Enabled	□	
▶ Network Password	••••••••	□	
▶ WPA Group Key Timeout	60 minutes	□	
▶ Interference Robustness	No	□	
▶ Channel	<<2 unique values>>	□	
▶ Multicast Rate	<<2 unique values>>	□	5.5
▶ Serve DHCP	Yes	□	
▶ Provide NAT	Yes	□	
▶ Radio Mode	802.11b/g Compatible	□	
▶ Transmit Power	1 mW	□	
▶ WAN Internet Connection	Ethernet	□	
▶ Configure WAN IP	DHCP	□	
▶ WAN DHCP Client ID		□	
▶ WAN IP Address	<<7 unique values>>	□	
▶ WAN Subnet Mask	255.255.0.0	□	
▶ WAN Router Address	0.0.0.0	□	
▶ Primary DNS Server	0.0.0.0	□	

Show: All

7 Base Stations selected

- If you don’t want to change the setting for all of the base stations in the group, click the triangle to the left of Multicast Rate to reveal all of the base stations in the group. Select the checkboxes in the New Setting column for the base station or base stations you want to change, double-click the new setting field, and enter the new value.

You can also click the triangle on the right and use the pop-up menu to choose a new value.



Name	Current Setting		New Setting
▶ Base Station Name	<<7 unique values>>	☐	
▶ Base Station Password	••••••••	☐	
▶ Base Station Contact	Morengo	☐	
▶ Base Station Location	<<7 unique values>>	☐	
▶ Base Station Firmware Version	<<3 unique values>>	☐	
▶ Network Name	PS404	☐	
▶ Closed Network	No	☐	
▶ Wireless Security Mode	Not Enabled	☐	
▶ Network Password	••••••••	☐	
▶ WPA Group Key Timeout	60 minutes	☐	
▶ Interference Robustness	No	☐	
▶ Channel	<<2 unique values>>	☐	
▼ Multicast Rate	<<2 unique values>>	⊟	<<2 unique values>>
SceiencLab (00:0d:93:81:31:3a)	2 Mbps	☑	5.5
Economics (00:0d:93:81:1d:4a)	2 Mbps	☐	
Sociology (00:0d:93:81:32:df)	2 Mbps	☐	
Biology (00:0d:93:81:23:66)	2 Mbps	☐	
Auditorium1 (00:0a:95:f1:d3:20)	1 Mbps	☑	11
ArtLab (00:0d:93:7d:3c:3b)	1 Mbps	☑	11
History (00:0a:95:f6:13:0c)	2 Mbps	☐	
▶ Serve DHCP	Yes	☐	
▶ Provide NAT	Yes	☐	
▶ Radio Mode	802.11b/g Compatible	☐	
▶ Transmit Power	1 mW	☐	

5 Click Apply to update the base stations with the new settings.

Adding a Second RADIUS Server

If you add a second RADIUS server to your network to back up an existing server or to accommodate more users of the network, you can update all of the base stations with the new settings for the second RADIUS server using AirPort Management Utility.

To update or add secondary RADIUS server information for all of the base stations in a group:

1 Open AirPort Management Utility.

2 Select the base station or the group of base stations you want to change.

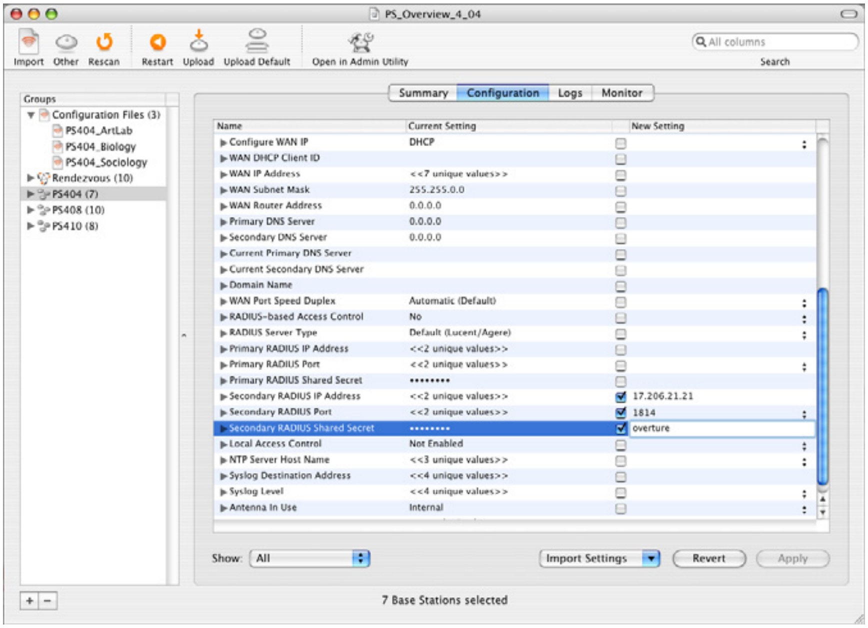
3 Click Configuration, and if prompted, enter the base station password. If the passwords for base stations in the group are different, you will be prompted for a password for each base station.

4 Select the Secondary RADIUS IP Address checkbox in the New Setting column, double-click the new setting field, and enter the IP address for the secondary RADIUS server.

5 Select the Secondary RADIUS Port checkbox in the New Setting column, double-click the new setting field, and enter the port for the secondary RADIUS server.

6 Select the Secondary RADIUS Shared Secret checkbox in the New Setting column, double-click the new setting field, and enter the shared secret for the secondary RADIUS server.

If you are changing the value for the entire group of base stations, make sure the triangle to the left of the secondary RADIUS settings is not pointing down.



Name	Current Setting		New Setting
▶ Configure WAN IP	DHCP	☐	
▶ WAN DHCP Client ID		☐	
▶ WAN IP Address	<<7 unique values>>	☐	
▶ WAN Subnet Mask	255.255.0.0	☐	
▶ WAN Router Address	0.0.0.0	☐	
▶ Primary DNS Server	0.0.0.0	☐	
▶ Secondary DNS Server	0.0.0.0	☐	
▶ Current Primary DNS Server		☐	
▶ Current Secondary DNS Server		☐	
▶ Domain Name		☐	
▶ WAN Port Speed Duplex	Automatic (Default)	☐	
▶ RADIUS-based Access Control	No	☐	
▶ RADIUS Server Type	Default (Lucent/Agere)	☐	
▶ Primary RADIUS IP Address	<<2 unique values>>	☐	
▶ Primary RADIUS Port	<<2 unique values>>	☐	
▶ Primary RADIUS Shared Secret	••••••••	☐	
▶ Secondary RADIUS IP Address	<<2 unique values>>	☑	17.206.21.21
▶ Secondary RADIUS Port	<<2 unique values>>	☑	1814
▶ Secondary RADIUS Shared Secret	••••••••	☑	overture
▶ Local Access Control	Not Enabled	☐	
▶ NTP Server Host Name	<<3 unique values>>	☐	
▶ Syslog Destination Address	<<4 unique values>>	☐	
▶ Syslog Level	<<4 unique values>>	☐	
▶ Antenna In Use	Internal	☐	

7 Base Stations selected

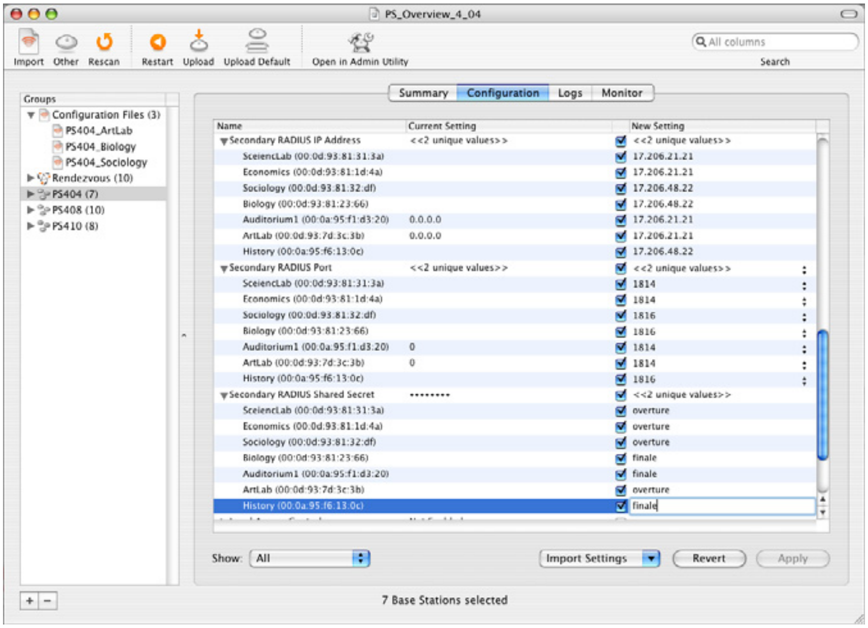
To add or update the secondary RADUIS settings for individual base stations in the group:

1 Select the group of base stations in the Groups list, then click Configuration. You may be asked for the base station passwords.

2 Click the triangle next to the secondary RADIUS setting you want to change.

3 Select the secondary RADIUS server checkboxes in the New Setting column for the base stations you want to change, and enter the new values.

4 Click Apply to send the new settings to the base stations.



Name	Current Setting		New Setting
▼Secondary RADIUS IP Address	<<2 unique values>>	☑	<<2 unique values>>
ScelencLab (00:0d:93:81:31:3a)		☑	17.206.21.21
Economics (00:0d:93:81:1d:4a)		☑	17.206.21.21
Sociology (00:0d:93:81:32:df)		☑	17.206.48.22
Biology (00:0d:93:81:23:66)		☑	17.206.48.22
Auditorium1 (00:0a:95:f1:d3:20)	0.0.0.0	☑	17.206.21.21
ArtLab (00:0d:93:7d:3c:3b)	0.0.0.0	☑	17.206.21.21
History (00:0a:95:f6:13:0c)		☑	17.206.48.22
▼Secondary RADIUS Port	<<2 unique values>>	☑	<<2 unique values>>
ScelencLab (00:0d:93:81:31:3a)		☑	1814
Economics (00:0d:93:81:1d:4a)		☑	1814
Sociology (00:0d:93:81:32:df)		☑	1816
Biology (00:0d:93:81:23:66)		☑	1816
Auditorium1 (00:0a:95:f1:d3:20)	0	☑	1814
ArtLab (00:0d:93:7d:3c:3b)	0	☑	1814
History (00:0a:95:f6:13:0c)		☑	1816
▼Secondary RADIUS Shared Secret	••••••••	☑	<<2 unique values>>
ScelencLab (00:0d:93:81:31:3a)		☑	overture
Economics (00:0d:93:81:1d:4a)		☑	overture
Sociology (00:0d:93:81:32:df)		☑	overture
Biology (00:0d:93:81:23:66)		☑	finale
Auditorium1 (00:0a:95:f1:d3:20)		☑	finale
ArtLab (00:0d:93:7d:3c:3b)		☑	overture
History (00:0a:95:f6:13:0c)		☑	finale

Changing the Network Password

If the security of your network has been compromised—someone leaked the network password, for example—you can reset the network password for all of the base stations that provide access to the network, and distribute that password to only those who require network clearance.

If network security is compromised, resetting the password as quickly as possible can restore network security and save valuable information from getting into the wrong hands.

To change the network password for all of the base stations in a group:

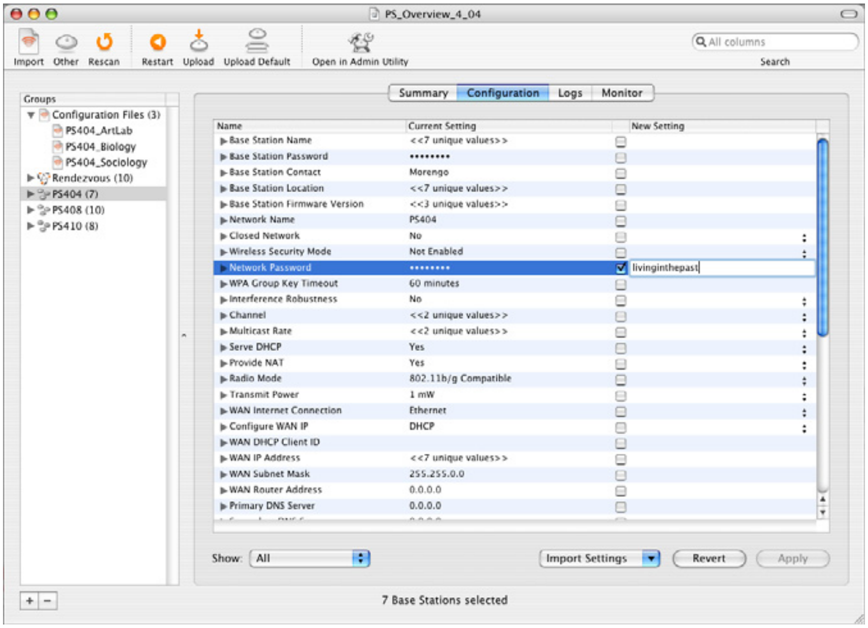
1 Open AirPort Management Utility.

2 Select the group of base stations you want to change in the Groups list.

3 Click Configuration, and if prompted, enter the base station password. If the passwords are different for the base stations in the group, you may need to enter for a password for each base station.

4 Select the Network Password checkbox in the New Setting column, double-click the new setting field, and enter the new password for the group.

5 Click Apply to send the new network password to every base station in the group.



Name	Current Setting		New Setting
Base Station Name	<<7 unique values>>	□	
Base Station Password	••••••••	□	
Base Station Contact	Morengo	□	
Base Station Location	<<7 unique values>>	□	
Base Station Firmware Version	<<3 unique values>>	□	
Network Name	PS404	□	
Closed Network	No	□	
Wireless Security Mode	Not Enabled	□	
Network Password	••••••••	☑	livinginthepast
WPA Group Key Timeout	60 minutes	□	
Interference Robustness	No	□	
Channel	<<2 unique values>>	□	
Multicast Rate	<<2 unique values>>	□	
Serve DHCP	Yes	□	
Provide NAT	Yes	□	
Radio Mode	802.11b/g Compatible	□	
Transmit Power	1 mW	□	
WAN Internet Connection	Ethernet	□	
Configure WAN IP	DHCP	□	
WAN DHCP Client ID		□	
WAN IP Address	<<7 unique values>>	□	
WAN Subnet Mask	255.255.0.0	□	
WAN Router Address	0.0.0.0	□	
Primary DNS Server	0.0.0.0	□	

Changing the Base Station Channel

If a new piece of equipment is installed near base stations on your wireless network, and it uses the same channel of the 2.4 GHz band as those base stations, connections to those base stations may be disrupted and network traffic and connections could fail. In mission-critical applications, such as wireless access to medical information, even temporary disruptions can be devastating. Even in less critical environments, such as a school network, poor network performance can hinder the educational experience for students or prevent staff from getting work done.

Fixing the problem could be as simple as changing the channel the affected base stations use.

To change the channel of base stations on your network:

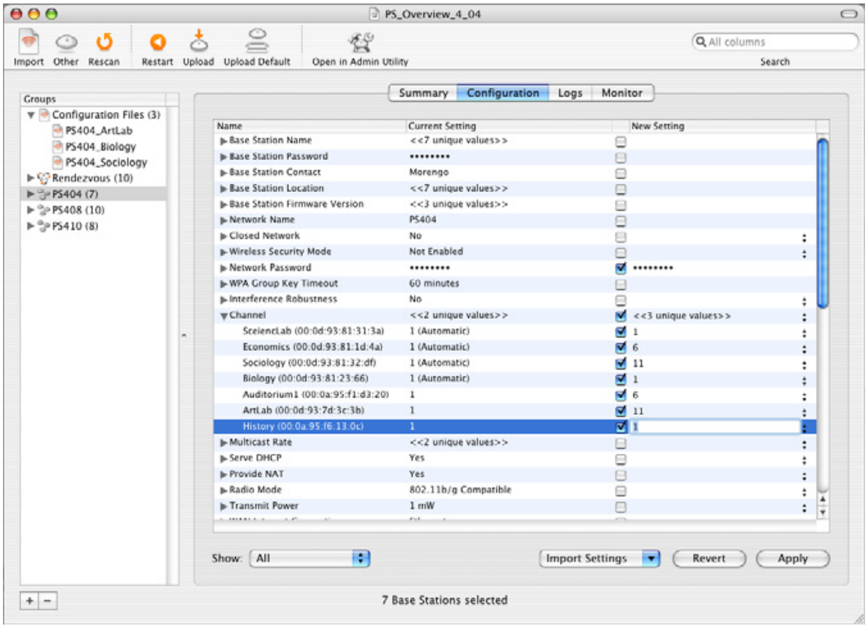
1 Open AirPort Management Utility.

2 Select the group of base stations in the Groups list and then select the base station in the group whose channel you want to change.

3 Click Configuration, and if prompted, enter the base station password.

4 Select the Channel checkbox in the New Setting column, double-click the new setting field, and enter a new channel.

Use the map from your site survey to identify base stations in adjacent rooms. Note their channels and try to select a channel that is separated by 3 or 4 channels. For example, if a base station in the next room is set to 6, try using channel 1 or 11 to avoid interference.



Name	Current Setting		New Setting
▶ Base Station Name	<<7 unique values>>	□	
▶ Base Station Password	••••••••	□	
▶ Base Station Contact	Morengo	□	
▶ Base Station Location	<<7 unique values>>	□	
▶ Base Station Firmware Version	<<3 unique values>>	□	
▶ Network Name	PS404	□	
▶ Closed Network	No	□	
▶ Wireless Security Mode	Not Enabled	□	
▶ Network Password	••••••••	☑	••••••••
▶ WPA Group Key Timeout	60 minutes	□	
▶ Interference Robustness	No	□	
▼ Channel	<<2 unique values>>	☑	<<3 unique values>>
ScienceLab (00:0d:93:81:31:3a)	1 (Automatic)	☑	1
Economics (00:0d:93:81:1d:4a)	1 (Automatic)	☑	6
Sociology (00:0d:93:81:32:df)	1 (Automatic)	☑	11
Biology (00:0d:93:81:23:66)	1 (Automatic)	☑	1
Auditorium1 (00:0a:95:f1:d3:20)	1	☑	6
ArtLab (00:0d:93:7d:3c:3b)	1	☑	11
History (00:0a:95:f6:13:0c)	1	☑	1
▶ Multicast Rate	<<2 unique values>>	□	
▶ Serve DHCP	Yes	□	
▶ Provide NAT	Yes	□	
▶ Radio Mode	802.11b/g Compatible	□	
▶ Transmit Power	1 mW	□	

7 Base Stations selected

Troubleshooting a Problem

The above examples are just some of the ways you can use AirPort Management Utility to help keep base stations on your network running efficiently. You can also use AirPort Management Utility to troubleshoot base station and network problems.

If you are administering a wireless network in a school, for example, and you receive a call from a teacher in a room where the wireless client computers are having problems connecting to the network through the base station in that room, you can use AirPort Management Utility to check the base station settings and make adjustments to try and solve the problem.

You can also monitor how many client computers are associated with the base station in the room, and check the signal quality and strength.

Here are some examples of using AirPort Management Utility to troubleshoot base station and wireless network problems.

In the Summary pane:

- Check the status of the base station in the Summary pane to make sure it is normal.
- Check the base station firmware version to make sure it is up to date.
- Make sure the base station has the correct IP address.

In the Configuration pane:

- Check the channel the base station is using. Use the facility map you annotated in your site survey, with base station locations, channel information, and power settings. Make sure the base station in question is not using the same channel as a nearby base station, and its power setting is correct.
- Check the value of the Closed Network setting. If the network is closed, it is hidden and client computers need to type the name of the network in order to join it.
- Check the Radio Mode setting. If the network is set to 802.11g Only, client computers with 802.11b wireless network cards will not be able to join the network.
- Check the Transmit Power setting. If the base station is in a large area, you may need to increase the power setting.
- Check the Wireless Security Mode setting. Make sure client computers are using the correct password or passphrase to join the network.
- Check the RADIUS settings. If your network is using RADIUS access control, make sure the client computers are using the correct RADIUS settings.
- Make sure the base station is set up to display logs. Use AirPort Admin Utility to set up the base station to display logs in AirPort Management Utility. See "Logging Base Station Messages" on page 39.

In the Logs pane:

- Check the base station log messages. See "Understanding Log Messages" on page 53 for more information about what the messages can tell you about the base station.
- Save the log messages as a text file, and send it to someone who may be able to help you understand more about the messages.

In the Monitor pane:

- Check the signal quality and strength of the wireless computer connected to the base station.
- Monitor the amount of noise the client computers are receiving.
- If only some client computers are reporting problems with their connection, you can identify them by the MAC address of the computer's wireless network card.
- Monitor the packet errors, and if possible, contact the teacher in the room to ask that the client computers experiencing problems move to another part of the room.

Additional Information

Here you'll find information about the log messages displayed in AirPort Management Utility, as well as items that can cause interference with your AirPort network.

Understanding Log Messages

Use the table below to help understand the base station log messages AirPort Management Utility displays in the Logs pane. The messages are separated by the severity level, set in AirPort Admin Utility.

Alert

Log Message	Description
sys: Now restarting.	The base station is now restarting.
admin: Begin soft reset mode.	The base station is in "soft reset" mode. The base station and network passwords will be reset to "public" for the next 5 minutes.
admin: End soft reset mode.	Soft reset mode has expired, and the base station has returned to normal function.
dot11: Begin TKIP countermeasures mode.	The base station has detected two TKIP message integrity check (MIC) errors within a 30-second interval, and has entered the "TKIP countermeasures" mode. All client computers have been deauthorized, and the base station will not allow client computers to join the network created by the base station for the next 60 seconds.
dot11: End TKIP countermeasures mode.	The "TKIP countermeasures" mode has expired, and the base station has returned to normal operation.
dot11: Error in TKIP integrity for station ${mac}.	The base station has received a report about a TKIP message integrity error in association with the client computer with the MAC address ${mac}.

Critical

Log Message	Description
: Undocumented software error ${code}.	An undocumented software error has occurred in the base station. (AppleCare may require the ${code} to assist with troubleshooting.)

Error

Log Message	Description
ntp: No network time server at ${address}.	The network time server with the IP address ${address} is unavailable. The base station may be presenting events with incorrect date and time. The ${address} field is either a numeric IPv4 address or a fully qualified Internet domain name.
ppp: Connection failed (${reason}).	The base station was unable to connect to the Internet using Point-to-Point Protocol (PPP) for the reason specified. The possible reasons are: • no PPPoE service • no modem interface • dial tone unavailable • call not answered • busy signal • carrier not negotiable • carrier lost
dhcpc: Configuration invalid (${progress})	The base station is unable to connect to the Internet using DHCP. This message is generated periodically while the base station continues to attempt to renew or reacquire its DHCP lease. Progress is described inside the parentheses as ${progress}. The possible values of ${progress} are: • in progress • giving up

Inform

Log Message	Description
admin: Parameter updated - ${parameter}	A base station setting has changed

Notice

Log Message	Description
sys: Initialized (firmware ${version} ${date})	The base station successfully started up and is ready for use. The version of firmware is ${version} and the date it was created is ${date}.
ether: Link down (${port}).	The link is down on the Ethernet port ${port}.
ether: Link up (${port} ${duplex} ${rate}).	The link is up on the Ethernet port ${port}. The status of the link is reported as half- or full- duplex and the rate is reported in megabits per second.
dot11: Session keys installed for station ${mac}.	The pairwise and group transient keys for the client computer with the MAC address ${mac} have been added to the base station and the client computer is now authorized to access the wireless network. This message is only presented in WPA Personal.
dot11: Group key rotated.	A new group key has been generated and added to the base station. All client computers are now required to negotiate the new group transient key.
dot11: Associated with ${mac}.	A new connection has been established with the wireless client computer with MAC address ${mac}.
dot11: Re-associated with ${mac}.	The connection has been re-established with the wireless client computer with MAC address ${mac}.
dot11: Disassociated with ${mac} (${reason}).	The connection with the wireless client computer with the MAC address ${mac} has ended for the specified reason. The possible reasons are as follows: • reserved ${numeric} • unspecified • authentication invalidated • leaving network • inactivity • received invalid class-2 frame • received invalid class-3 frame • leaving service set • not authenticated • bad power capability • bad channel capability • bad security Information element • message integrity error • 4-way timeout • group key timeout • 4-way protocol error • bad multicast cipher • bad unicast cipher • bad key management protocol • bad security capabilities • 802.1X authentication failed

Log Message	Description
ppp: Connecting to dialup ${telephone} (user "${user}”).	The base station is initiating a connection to the Internet over the modem interface using dial-up PPP to the telephone number ${number} using the user account ${user}.
ppp: Connecting via ethernet (user “${user}” service “${service}”).	The base station is initiating a connection to the Internet over the Ethernet interface using PPPoE with the user account ${user} at the service named ${service}.
ppp: Connection established ${local} -> ${remote} (dns ${dns}).	The base station is now connected to the Internet using PPP at the Internet address ${local}. Its remote peer is at the Internet address ${remote}, and its Domain Name Service (DNS) resolving proxies are located at the Internet addresses listed by ${dns}. All Internet addresses are presented in numeric form. The list of DNS proxies is either a single address or a pair of addresses separated by a space character.
ppp: Disconnected.	The base station has disconnected from the Internet using PPP.
dhcpc: Internet configuration leased (host ${host}/${subnet} gateway ${gateway} dns ${dns} domain ${domain}).	The base station has obtained a DHCP lease for access to the Internet. Its address is ${host} on a subnet with a mask of length ${subnet}, and its default gateway is ${gateway}. Its Domain Name Service (DNS) resolving proxies are located at the Internet addresses listed by ${dns}, and its default domain name suffix is ${domain}. All Internet addresses are presented in numeric form. The list of DNS proxies is either a single address or a pair of addresses separated by a space character.
admin: Connection accepted from ${address}:${port}.	The base station has accepted an administrative connection from a client computer at the address ${address} and TCP port number ${port}. The client address is presented as a numeric IPv4 address.
admin: Configuration updated.	The configuration of the base station has been updated.
ntp: Clock synchronized to network time server ${address}.	The base station has synchronized its clock with the network time server at the address ${address}. The address may be reported as a numeric IPv4 address or as a fully qualified domain name.

Warning

Log Message	Description
admin: Administrative access denied to ${address}	An attempt to access the AirPort Management Utility was denied to the client computer at ${address} because the user name was not recognized. The ${address} field is a numeric IPv4 address followed by a TCP port number.
dot11: Authentication failed for station ${mac}.	The client computer with the MAC address ${mac} is not listed in the base station's fixed-address access control list.
dot11: Bad pre-shared key at station ${mac}.	The client computer with the MAC address ${mac} is using the wrong passphrase for the wireless network. This message is only presented in WPA Personal mode when the specified client computer is not performing the 802.11i "four-way handshake" correctly, or in WEP mode (both 40-bit and 104-bit) when the client computer is not using the correct WEP key.
dot11: Bad pairwise master key at station ${mac}.	The client computer with the MAC address ${mac} is negotiating with the wrong pairwise master key for the secure wireless network. This message is only presented in WPA Enterprise mode when the specified client computer has authenticated successfully to the authorization server, but is not performing the 802.11i "four-way handshake" correctly.

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 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 higher.
- Moving objects that temporarily place metal between your computer and the base station

019-0153