PLANEX COMMUNICATIONS

Installation and Configuration Guide

108 Mbps Wireless Access Point CQW-AP108AG

Planex Communications
Head Quarters-Japan
PCI Building
12-7, Nihombashi Odemma-cho, Chuo-ku
Tokyo, 103-0011
www.planex.co.jp

Published: July 2004

プラネックスコミュニケーションズ、PLANEX　COMMUNICATIONSはプラネックスコミュニケーションズの登録商標です。

Contents

Preface

This guide explains how to install and configure the 108 Mbps Wireless Access Point (108 Mbps Wireless AP), which is used with Wi-Fi certified clients to provide PC laptop and desktop users with wireless network access.

The 108 Mbps Wireless Access Point provides the following features:

- High throughput and range through dual-band radio transceivers
- Easy installation
- Wireless networking features that include bridging, VLAN, Quality of Service (QoS), IP routing, and network backhaul capabilities
- Comprehensive security that includes support for WEP, TKIP, AES, EAP-PEAP, EAP-TLS, and RADIUS
- Automated radio resource management, including controls for operating channels, capacity, and range
- Policy-based management

Audience

This guide is designed to help you install and configure the 108 Mbps Wireless Access Point successfully even if you are unfamiliar with wireless networking technology. Some familiarity with local area networking technology is assumed. If you encounter a term or acronym with which you are unfamiliar, refer to the glossary at the end of the guide, just before the index.

Organization of this Guide

This guide consists of the following chapters:

- **Chapter 1, "Overview,"** provides a high-level overview of the 108 Mbps Wireless Access Point products.
- **Chapter 2, "Planning Your Installation,"** describes various deployment scenarios and helps determine how many 108 Mbps Wireless Access Points will be needed and the appropriate network management scheme.
- **Chapter 3, "Installing the Access Point,"** describes how to install the 108 Mbps Wireless Access Point and how to use the Quick Start panels for fast and easy configuration. Also explains how to use the 108 Mbps Wireless AP web interface.
- **Chapter 4, "Configuring Radio Settings,"** explains how to configure the 108 Mbps Wireless Access Point radios.
- **Chapter 5, "Configuring Networking Settings,"** explains how to configure the advanced networking features of the 108 Mbps Wireless Access Point.
- **Chapter 6, "Configuring a Wireless Backhaul,"** explains how to use the wireless backhaul feature to configure a wireless distribution system that can cover a large area with limited wired network connectivity.
- **Chapter 7, "Managing Security,"** describes the encryption and authentication features of the 108 Mbps Wireless Access Point and explains how configure the security options.

- **Chapter 8, “Configuring Guest Access,”** describes how to configure guest access for the network.
- **Chapter 9, “Managing the Network,”** explains how to use the NM Portal features of the 108 Mbps Wireless Access Point to manage multiple APs across your network.
- **Chapter 10, “Maintaining the Access Point,”** describes the tools available to maintain the 108 Mbps Wireless Access Point.
- **Appendix A, “Using the Command Line Interface,”** describes how to use the console and command line interface (CLI) to configure the 108 Mbps Wireless Access Point, with cross-references to the PLANEX Command Line Interface Reference Manual.
- **Appendix B, “Regulatory and License Information,”** provides regulatory specifications. for the 108 Mbps Wireless Access Point.
- **Appendix C, “Alarms,”** provides a description of the alarms generated by the 108 Mbps Wireless Access Point.
- **Glossary**— Provides definitions for acronyms, networking terminology, and PLANEX-specific terms.

Conventions Used in this Guide

This guide uses the following conventions for instructions and information.

Notes, Cautions, and Warnings

Notes, cautions, and time-saving tips use the following conventions and symbols.

NOTE: Notes contain helpful suggestions or information that may be of importance to the task at hand.

CAUTION: Caution indicates that there is a risk of equipment damage or loss of data when certain actions are performed.

WARNING: Warnings are intended to alert you to situations that could result in injury (such as exposure to electric current, for example).

Command Conventions

Table 1 describes the command syntax used in this document.

Table 1:Command Conventions

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Optional keywords and default responses to system prompts appear within square brackets.
{**x** | **x** | **x**}	A choice of keywords (represented by **x**) appears in braces separated by vertical bars. You must select one.
Ctrl	Represents the key labeled *Ctrl*. For example, when you read *^D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`panel font`	Examples of information displayed on a panel.
`boldface panel font`	Examples of information the user must enter.

Related Documentation

The following documentation related to the PLANEX wireless networking product line is available on CD-ROM and also on the PLANEX website, http://www.planex.co.jp.

- **PLANEX 108 Mbps Wireless LAN PC Card (CQW-NS108AG) Installation and Users Guide** — Explains how to install and configure the PLANEX Wireless LAN Client Adapter, which provides PC laptop and desktop users with access to the PLANEX Access Point products.
- **PLANEX Wireless LAN Network Management Software Installation and Configuration Guide** — Explains how to use PLANEX Wireless LAN Network Management Software to manage an enterprise wireless network.
- **PLANEX Command Line Interface (CLI) Reference Manual** — Provides a listing of all the commands available for PLANEX wireless products through serial console access and the command line interface. Intended for advanced users and system administrators.

1 Overview

This chapter introduces the features and capabilities of the 108 Mbps Wireless Access Point and presents the following topics:

Product Overview

The 108 Mbps Wireless Access Point is part of an innovative suite of wireless technology products designed to dramatically improve the quality and convenience of wireless networking. By greatly increasing the range, speed, reliability, security, and ease-of-use of wireless LAN (WLAN) systems, PLANEX products help to promote the mainstream adoption of wireless technology, and help to foster new wireless applications.

Product Suite

The PLANEX product suite comprises these wireless networking products:

- 108 Mbps Wireless Access Point
- 108Mbps Wireless LAN PC Card
- PLANEX Professional Network Management System (Wireless LAN Network Management Software)

108 Mbps Wireless Access Points

108 Mbps Wireless Access Points (108 Mbps Wireless AP) provide network connectivity for wireless client stations. Incorporating the latest technological advances in radio design and implementation, the dual-radio 108 Mbps Wireless Access Point offers very high wireless performance, financial-grade security, and extended wireless coverage.

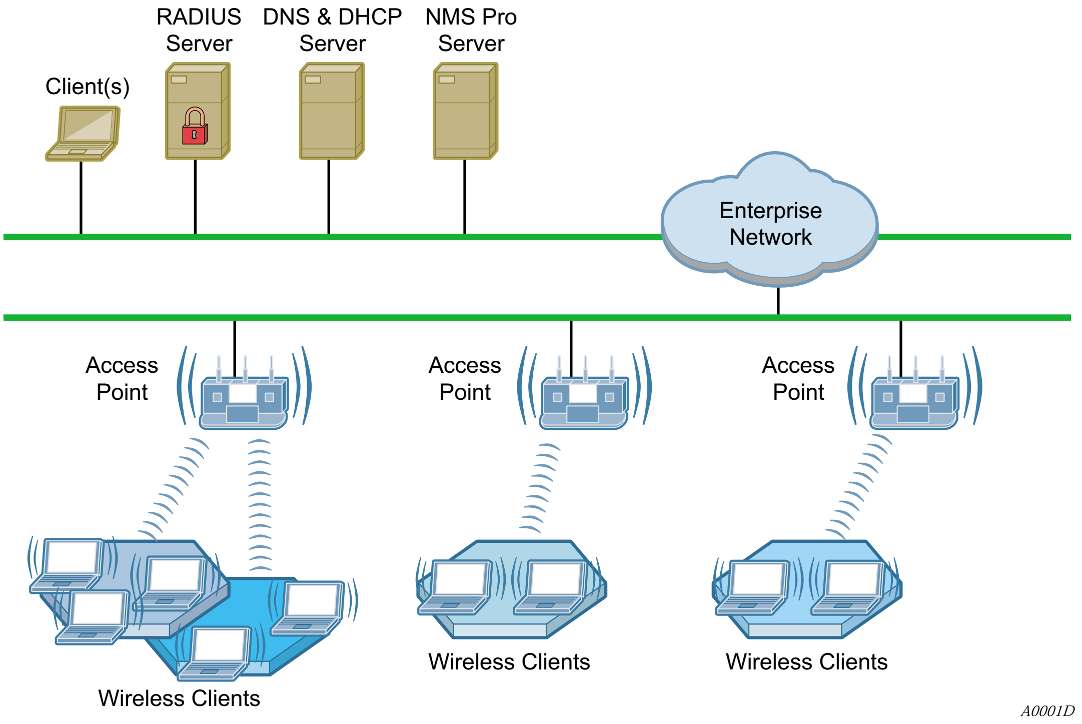
108Mbps Wireless LAN PC Card

The 108Mbps Wireless LAN PC Card provides the communications link between laptop or desktop PC users and wireless network. Available in PC Card and Mini PCI Card form factors, the 108Mbps Wireless LAN PC Card is designed to take full advantage of the performance, range, security, and management capabilities of the 108 Mbps Wireless Access Point. For more information, refer to the *108Mbps Wireless LAN PC Card Installation and User Guide.*

PLANEX Wireless LAN Network Management Software
PLANEX's Wireless LAN Network Management Software provides enterprise-class management for the wireless network, including complete configuration and image control, security, and performance and fault monitoring. For more information, refer to the *Wireless LAN Network Management Software Installation and Configuration Guide.*

Figure 1 shows how PLANEX products operate in concert to create a wireless network.

Figure 1: PLANEX Wireless Network



Features Overview

108 Mbps Wireless Access Points extend the range, coverage, and bandwidth of traditional wireless equipment, while also supporting the latest network security and management features. All 108 Mbps Wireless Access Point models include the following features:

- Dual radios, each operating in 802.11b/g or 802.11a mode
- Optional PLANEX enhanced data rates up to 108 Mbps
- Automated frequency management
- Cell size and range management
- Support for all current IEEE 802.11 standards and draft versions of 802.11 standards
- Multiple SSID support
- Bridging, including layer 2 filtering, encapsulation modes, 802.1x support, and static forwarding
- Easy installation and configuration
- Single and multiple VLAN support, interface-based and user-based
- 802.11 roaming support
- Web and command line user interfaces

- Embedded Network Management and Security Portal services
- Financial grade security
- Effective security management
- Guest user access
- Rogue AP detection
- Quality of service (QoS)
- Wireless backhaul modes
- Integration with existing wired network infrastructure
- Static IP routing
- SNMP MIB support
- Authentication using RADIUS services
- Software and firmware upgrades
- Back up and restoration of AP configuration data
- SYSLOG and diagnostic tools for monitoring and troubleshooting

Radio Resource Management

The 108 Mbps Wireless AP supports management of radio channels, cell size, and range.

Channel management features include automatic channel selection, support for international channel sets, dynamic channel changes in response to network conditions, and the ability to assign channels manually to fine tune channel quality. Cell size and range capabilities enable you to optimize equipment placement, eliminate dead spots, and reduce interference.

Mobility Management

Mobility management features include Layer 2 roaming (as users move from one coverage area of an access point to another or are switched for load balancing purposes), quality of service support, and comprehensive security features. The 108 Mbps Wireless AP also provides support for 802.11f based Inter-Access Point Protocol (IAPP).

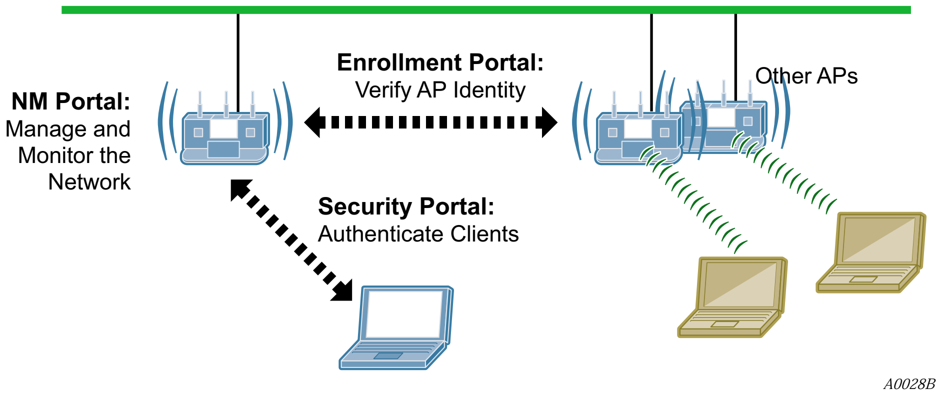
Portal Architecture

To support the range of network sizes and configurations served by PLANEX products, PLANEX has designed a built-in, flexible, portal services architecture for management and security. Each AP can be configured as an *NM Portal AP* to support the following services:

Service	Description
Management	NM Portal services provide network management functionality for small to mid-size wireless networks. Each 108 Mbps Wireless AP configured as an NM Portal can operate in stand-alone mode to provide network management for the entire network or as a location or branch manager working in conjunction with Wireless LAN Network Management Software, the PLANEX Professional Network Management System.
Security	Security portal services include support for secure user authentication by way of a RADIUS server internal to the 108 Mbps Wireless AP. Security portal services are part of NM Portal, but can also be configured independently for backup authentication in the event that the primary internal RADIUS server becomes unavailable.
Enrollment	Each PLANEX wireless network requires an enrollment server to verify the identity of 108 Mbps Wireless APs and authorize them for operation in the network. The enrollment portal feature is automatically enabled in the access point as part of NM Portal. NM Portal should be used for enrollment unless Wireless LAN Network Management Software has been implemented as the enterprise network management solution.

Figure 2 illustrates portal services within the PLANEX network. NM Portal provides overall network management functionality and monitoring. The enrollment portal feature enables verification of additional APs and authorization for operation in the network. The security portal feature verifies the identity of individual users wanting access to the network.

Figure 2: Portal Services



Regardless of network size, configuring one or more 108 Mbps Wireless APs as NM Portals yields the following benefits:

- Even with as few as two APs in a network, NM Portal offers a single point of focus for monitoring the network and managing security. Configuring the first AP as an NM Portal makes it easy to enroll additional APs.

- The configuration of the NM Portal AP is easily distributed to the other APs in the network, assuring consistent application of configuration parameters.
- NM Portal can provide user authentication services for an entire small to mid size network or serve as a backup security server if an external RADIUS authentication service is used.

Security

PLANEX offers a comprehensive security solution that adheres to the following industry standards and draft standards:

- Data encryption—WEP, Wi-Fi Protected Access (WPA) with TKIP or AES encryption
- User authentication—IEEE 802.1x authentication, including EAP-PEAP or EAP-TLS; WPA-PSK
- Key management—Microsoft-IAS, FUNK-RADIUS, PLANEX Wireless LAN Network Management Software, PLANEX integrated security portal, and manual key management capabilities

These features are part of a security architecture that provides the wireless network a greater degree of security than most traditional wired networks. The following security features are included with all 108 Mbps Wireless AP:

- Built-in maximum industry-standard security
- Auto-detection of the security capability of clients and APs
- Policy-based configuration of security settings
- Hardware support for high-performance encryption
- Support for installations ranging from the small-office/home-office (SOHO) to multi-site enterprises
- Command-line access using SSH (secure shell)
- Web-based management interface and policy-based management using HTTPS (SSL)
- SNMP management interface through SNMPv3
- IEEE 802.11i standards
- User-authentication using EAP-TLS, EAP-PEAP, WPA-PSK, WEP
- Rogue AP detection
- Rogue client detection

VLANs

By decoupling traffic flow and network services from the physical network topology, virtual LANs (VLANs) enable enterprises improve network traffic flow, increase load, and deliver varying levels of service and access to different groups of users. The 108 Mbps Wireless AP VLAN feature readily extends an existing wired VLAN structure to the wireless network. It can also be used to implement new network privileges and services; for example, user VLANs are integral to the PLANEX guest access feature (see “Guest Access” on page 6).

PLANEX supports interface-based VLANs and user-based VLANs. Interface VLANs separate traffic according to the Ethernet and radio interfaces on the 108 Mbps Wireless AP. Packets destined for a specific interface VLAN are directed to the port with that VLAN assigned. By contrast, user VLANs separate traffic according to user groups. Users can be assigned to the same VLAN even if they are in different physical LANs and at geographically dispersed locations. User VLANs are useful for managing manage enterprise work groups and differentiating among categories of users. The 108 Mbps Wireless Access Point supports up to 16 VLANs, including a default VLAN.

Quality of Service

Quality of Service (QoS) features enable differential treatment of network traffic types to support special applications or extend priority access to designated groups of users. For example, applications as streaming media and voice over Internet suffer serious quality degradation if data transmission is interrupted or bandwidth fluctuates excessively. You can assign a higher quality of service to applications of this type, while still maintaining adequate service for less intensive applications such as print and file sharing. Network utilization is increased with little to no negative effect on user productivity. QoS can also be used to lower the priority for non-critical applications. For example, FTP transfers, which are generally not time critical but can consume significant network bandwidth, can be assigned lower priority than streaming media applications or database transactions.

QoS can also be assigned on a user group basis. For example, network administrators can be assigned a higher quality of service than other employees, thereby enhancing their ability to manage and troubleshoot a heavily loaded network.

PLANEX implements quality of service features using classes of service (COS). Eight COS levels are available for assignment according to user or application based rules. The COS approach does not guarantee bandwidth, but it does give “best effort” priority according to the assigned level. A flexible approach to service quality, it scales easily and accommodates a variety of mapping rules. MAC layer mappings for COS levels and COS to IP layer mappings are supported, and priority settings can be assigned for different COS mapping rules.

IP Routing

IP routing adds flexibility to AP management and expands the addressing capability of the AP. You can specify static IP addresses outside the local subnet along with routing information to reach the addresses.

Multiple SSIDs

The 108 Mbps Wireless AP supports multiple SSIDs within each individual AP. Using the multiple SSID feature, users can access separate networks through a single physical infrastructure. For example, if you want to create different levels of resource access for employees and visitors, you can create two SSIDs, one with high security and one with open security.

Guest Access

The 108 Mbps Wireless AP supports flexible, secure managing of guest access at corporate locations. By contrast with most other guest access solutions, the 108 Mbps Wireless AP supports guest access without requiring any changes to the physical network topology. VLAN tags on the existing access points segregate users into corporate and guest VLANs, and guests are automatically directed to an internal or external web landing page. Guest passwords can be assigned statically or change dynamically according to a pre-set schedule. An open access option is available to provide unauthenticated guests with access to an open subnet.

Rogue AP Detection and Classification

Maintaining a secure wireless network requires ongoing monitoring of potential rogue access points and the ability to classify them as known to the local or neighboring network, or as true rogues. The network management functions of NM Portal include automatic network scanning and display of all the detected APs that potentially qualify as rogues. Using the information included in the display, network administrators can identify and classify the APs that are known. The remaining APs are classified as rogues. By examining the information available for each rogue AP, it is generally possible to pinpoint the location of the rogue and take action to remove it from the network.

Standards and Data Rates

PLANEX supports the wireless networking standards shown in Table 2.

Table 2: Supported Wireless Networking Standards

Standard	Area	Status
IEEE 802.11b	Wireless LAN	Approved Standard
IEEE 802.11a	Wireless LAN	Approved Standard
IEEE 802.11g	Wireless LAN	Approved Standard
IEEE 802.11d	World Mode Support	Approved Standard
IEEE 802.11e	HCF & eDCF	Draft Standard
IEEE 802.11f	Inter-AP Protocol (IAPP)	Draft Standard
IEEE 802.11h	TPC and DFS additional regulatory domains	Approved Standard
IEEE 802.11i	Wireless Security	Approved Standard
IETF Standards	Security EAP-TLS	Draft Standard
Microsoft Standard	Security EAP-PEAP	Draft Standard
IETF SNMP MIBs	Numerous RFC MIBs	Standard
IETF Protocols	Bridging, Routing	Standard
WPA	Security Standard	Standard
Wi-Fi Alliance	Wireless Interoperability	Certification

The 802.11 standard specifies the following data rates:

- 802.11b: DSSS (1, 2, 5.5 and 11 Mbps)
- 802.11a: OFDM (6, 9, 12, 18, 24, 36, 48, 54 Mbps)
- 802.11g: OFDM (6, 9, 12, 18, 24, 36, 48, 54 Mbps)

PLANEX also offers enhanced data rates of 72, 96, and 108 Mbps for enhanced performance.

Integration With the Existing Wired Network

PLANEX wireless networking solutions are standards-compliant to ensure seamless integration with existing wired network infrastructures. The following integration features are included with all 108 Mbps Wireless APs:

- 10/100 Ethernet connectivity
- 802.1Q VLAN support
- 802.1p QOS support
- 802.3af Power-over-Ethernet support
- Layer 2 and Layer 3 QoS support
- DHCP server and client support
- NTP for time-synchronization

Management Interface Options

Management support for the 108 Mbps Wireless AP is available through four different interfaces:

Interface	Description
Web Browser Interface	This is the primary user interface for basic and advanced AP configuration support for a single AP. This guide presents all configuration tasks using the web browser interface.
NM Explorer	A built-in NM Portal web interface is available to manage multiple APs. For details on using NM Portal, see Chapter 9, "Managing the Network."
Command Line Interface (CLI)	The command line interface (CLI) for the 108 Mbps Wireless AP is accessible through a local 9-pin serial console port or over SSH. For more information on using the CLI to configure the AP, see Appendix A, "Using the Command Line Interface."
Wireless LAN Network Management Software	The Wireless LAN Network Management Software user interface provides access to AP configuration functions and is designed to manage very large numbers of access points and networks. For more information, see the *Wireless LAN Network Management Software Installation and User Guide*.

2 Planning Your Installation

This chapter provides guidelines on planning a wireless network. It includes example network configurations and explains how to plan for coverage, capacity, security, and network management. The chapter includes the following topics:

Introduction

Careful planning of a new wireless network can greatly enhance your ability to install, maintain, manage, and expand the network. There are several dimensions to installation planning:

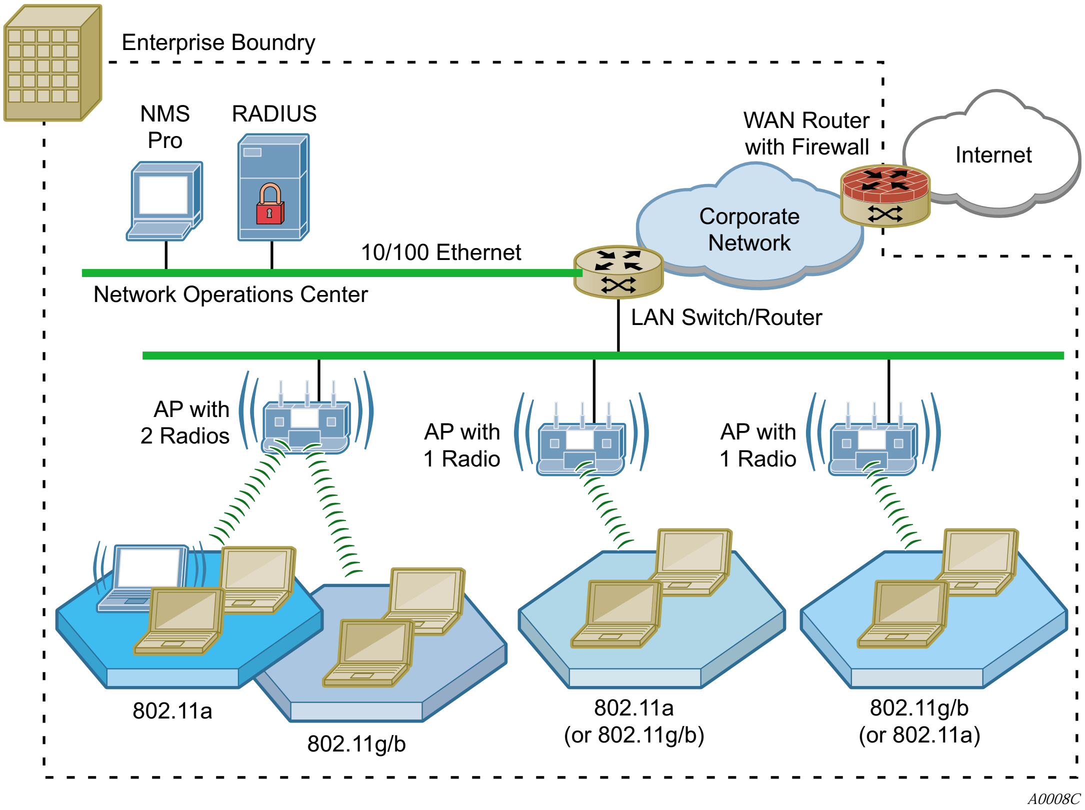
- Coverage and capacity requirements—Identify the numbers and types of access points to install and determine optimal placement.
- Security needs—Choose a security architecture and features.
- Network management—Choose a method to manage the network and monitor its health.
- Network features—Determine VLAN assignment, user groups, services, and privileges.

If planned properly, a wireless network can be easily expanded and adjusted to changing conditions and requirements while preserving effective security and enabling network-wide management support.

Example Wireless Network Installation

Figure 3 shows the elements of a typical PLANEX wireless network. 108 Mbps Wireless Access Points provide wireless connectivity to client stations (laptop or desktop computers) and connect in turn to the existing wired network infrastructure and beyond to the Internet. Network size and complexity may also dictate the need for an external RADIUS server for user authentication, as well as installation of PLANEX Wireless LAN Network Management Software for enterprise network management.

Figure 3: Typical Wireless Network

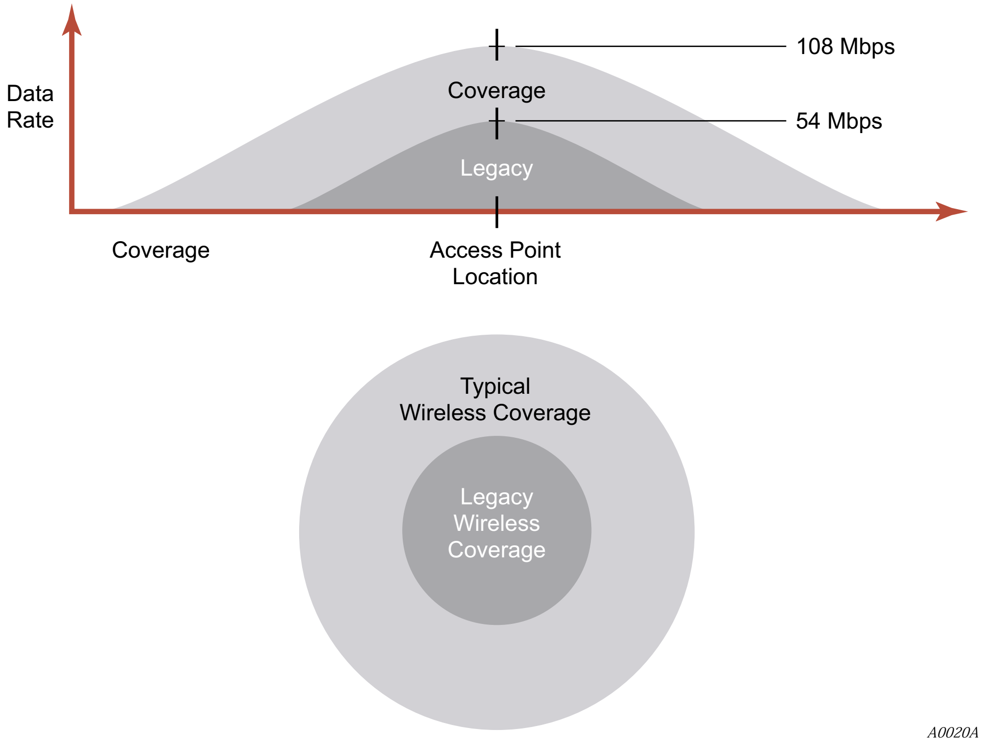


Assessing Coverage and Capacity Requirements

PLANEX wireless technology significantly increases wireless coverage or capacity by comparison with other wireless LAN products. This wireless advantage allows an access point to service a large area or provide higher data rates, depending upon the conditions at your location. Figure 4 illustrates the contrast between typical wireless coverage and PLANEX wireless coverage. Each 108 Mbps Wireless AP can service a wider area or provide higher data rates than alternative solutions.

Precise coverage and capacity vary considerably depending on factors such as the specific 802.11 protocol being used, antenna placement and location, building construction materials, and local obstructions.

Figure 4: 108 Mbps Wireless AP Coverage Compared with Other Access Points



Site Surveys

Site surveys are used to measure the wireless characteristics of the physical environment and thereby determine cost-efficient placement of equipment in the network. They are important because the physical attributes of a location may have a significant impact on realized coverage and data rates. The site survey involves a detailed assessment of the radio signal environment of the site based on experiments and testing. After the wireless network equipment is installed, radio signals are sent between the AP and a mobile client (laptop) to effectively tune the placement of APs.

A professional site survey is highly recommended for large installations, but can be an expensive and time-consuming process, especially for installations with a variety of buildings and building materials, radio signal conditions, and restrictions on equipment placement. Thanks to the dramatic improvements in capacity and coverage provided by 108 Mbps Wireless APs, many small to mid-size companies can forgo the traditional site survey process and rely instead on general guidelines.

Assessing Security Needs and Architecture

The latest security innovations and standards make it possible to provide complete and effective security for wireless networks. The specifics of an optimal security solution will vary according to the type and size of organization. For each environment, PLANEX offers a selection of features to satisfy all your security needs.

Three aspects of security require planning and decisions:

- Enrollment—Specifying the 108 Mbps Wireless AP or Wireless LAN Network Management Software server used to verify which access points are authorized to be part of the wireless network.

- Data encryption—Specifying the method of security for wireless data communications between client stations and the AP.
- Authentication—Specifying the method to verify the identity of users who want to access the wireless network, and assign access restrictions and services to them.

Enrollment

Enrollment is the process of verifying the identity of APs and confirming that they are authorized to be a legitimate part of the wireless network. It is recommended to designate a single enrollment server for the entire network. For small and mid-size networks, this should be an AP configured as an NM Portal (see “Selecting a Network Management Method” on page 13). For large offices and campuses, it is recommended to use the enrollment module within Wireless LAN Network Management Software as the enrollment server. The process of enrollment is discussed in “Enrolling APs” on page 167.

Data Encryption

Data encryption is the process whereby data packets are encoded to prevent intruders from deciphering the content. The first wave of IEEE 802.11 products introduced encryption based on the Wired Equivalent Privacy (WEP) standard. The WEP algorithm uses keys configured on the AP and in the user client software to encrypt wireless data. Unfortunately, WEP is vulnerable to compromise and difficult to manage and configure. Temporal Key Integrity Protocol (TKIP) is the secure successor to WEP.

The current state of the art for data encryption is the Advanced Encryption Standard (AES), adopted by the Wi-Fi Alliance as part of the IEEE 802.11i working group efforts and grouped under the heading Wi-Fi Protected Access (WPA). The new IEEE 802.11i standard provides financial-grade security with extremely strong AES over-the-air encryption. The keys used for every user session are unique and are established automatically using the IEEE 802.1x protocol.

Unless your wireless network must support WEP encryption, using WPA with AES for data encryption, regardless of your network size or complexity, is recommended.

User Authentication

User authentication is the process of verifying user identity and assigning access rights based on predetermined rules. For small to mid-size networks, the internal RADIUS server within the 108 Mbps Wireless AP security portal provides authentication services across the network. A second AP can also be configured as a backup security portal.

For large office and campus installations, one or more external RADIUS authentication servers may already be in place to provide authentication services for the wired network based on the IEEE 802.1x RADIUS standard. It is a straightforward exercise to extend that infrastructure to the wireless network, thereby creating an integrated user authentication process for the entire enterprise network.

The security portal feature of the 108 Mbps Wireless AP plays a special role in wireless backhaul authentication. For more information, see Chapter 6, “Configuring a Wireless Backhaul.”

Selecting a Network Management Method

As with user authentication, appropriate network management solutions depend upon the size and complexity of the network, and PLANEX products and features are available to support the full range of possibilities.

For small and mid-sized networks, it is recommended to configure one of the APs on the network as a portal AP to provide NM Portal, security portal, and enrollment services. It is also recommended to designate another AP as a backup for the security portal.

For large offices and campuses, enterprise-wide control and advanced network management features become essential to reliable network operations. For these networks, it is recommended to use the PLANEX Wireless LAN Network Management Software network management application, which provides a comprehensive network management solution. Install the Wireless LAN Network Management Software server on any suitably configured network computer, and permit network administrators to obtain access from any designated client station. For more information, see the *PLANEX Wireless LAN Network Management Software Installation and Configuration Guide*.

Wireless LAN Network Management Software can be installed as a stand-alone network management solution, or it can be used in conjunction with NM Portal APs to create an efficient distribution system for network management data and policies across multiple locations. For enterprises with multiple locations, an AP in each location can be assigned as the NM Portal. The NM Portal serves an auxiliary function, executing commands for AP management updates and distributing them to all the APs at the remote location or collecting data from all the APs at the location and sending the data back to Wireless LAN Network Management Software. This model can significantly reduce the time and network load associated with performing network management functions such as policy distribution and software updates.

Planning Network Features

The 108 Mbps Wireless AP offers an extensive set of configuration parameters and network service features. Automated and default options are available for most of these, making it necessary to configure only a few of the AP parameters to set up a basic network. As needs change, additional features can be configured to support new network services.

Network feature planning involves the following decisions:

Feature	Planning Issues
Physical Network	Estimate how many APs are expected initially and with growth. Determine whether wireless backhaul will be required.
Network Management	Determine the network management structure. • A network management solution such as NM Portal or Wireless LAN Network Management Software is strongly recommended for all multiple AP installations. • NM Portal is recommended for small to mid-size networks. • Wireless LAN Network Management Software is recommended for large enterprise networks. Wireless LAN Network Management Software can be used in conjunction with NM Portal for an efficient, hierarchical network management solution. • If wireless backhaul is selected, then network management must include NM Portal.
Authentication	Determine how to verify the identity of users requesting access to the network. An authentication scheme is required for all except Open access. • **Pre-shared key (PSK) authentication** uses matching keys assigned prior to the authentication session and stored on the AP and in the client. With PSK, no external authentication server is required. This approach is useful for small to mid-size networks in which keys can be easily configured and modified, as needed. • **RADIUS user authentication** relies upon individual login and password. This approach is preferred for medium-large and enterprise networks that must accommodate large, changing user populations. RADIUS is the most common protocol used in authentication servers. The 108 Mbps Wireless AP can take advantage of the authentication services provided by an external third party RADIUS server, or the internal RADIUS security portal on the 108 Mbps Wireless AP can be used. In conjunction with an external RADIUS server, the security portal provides wireless backhaul authentication services and can serve as a back-up authentication server if the external RADIUS server is not available. An authentication zone is a group of one or more RADIUS servers providing user authentication services within an SSID. If multiple SSIDs are configured, then you can create an authentication zone for each. The chosen authentication method influences how services can be configured in the network.

Feature	**Planning Issues**
Security Modes	Choose WPA, WEP, or open security modes. • WPA is recommended, unless WEP is required for communication with legacy systems. • WPA security is compatible with WEP and with open security. WEP is not compatible with open security. • Guest access requires the open security mode. • The preferred encryption method is AES, unless TKIP or WEP are required for compatibility with legacy systems.
VLAN	VLANs permit the network to be segmented according to functional needs without the restrictions of the physical topology. • If your enterprise uses multiple VLANS, they can be supported in the wireless network. • Multiple VLANs are required for guest access.
SSID	Decide whether one or multiple SSIDs will be supported. • Multiple SSIDs are desirable for applications such as wireless Internet service (WISP), in which a single physical access point supports multiple user populations in distinct networks. • Multiple SSIDs permit support of multiple service levels in networks that rely on PSK rather than user-based authentication. Services are bound to the SSID rather than to specific user groups.
Quality of Service	Quality of Service (QoS) allows you to set priorities for user traffic, thereby increasing the likelihood that critical data will obtain the needed priority. QoS is implemented by way of class of service (COS) mappings. Accept the default mappings or define custom mappings to create special high or low priority classes of service. • Default and custom mappings are compatible with other feature selections.
Service Profile	Service profiles specify the services available for an SSID or for designated user groups within an SSID. Accept the default service profile or create custom service profiles to provide varying levels of service. The service profile includes VLAN assignment, COS, and minimum security. Once created, a service profile can be bound to an SSID with or without a specified user group. • If a user group is included in the binding of a service profile to an SSID, then members of the user group are automatically assigned that profile when authenticated. • If no user groups are specified, then all users who access the SSID are assigned the same profile.
Guest Access	Guest access refers to special treatment of users who are not authorized to access the main corporate network. The guest access feature allows non-authorized users to gain network access in a controlled way. Decide whether the network will support guest users and if so, how guest access will be managed. • Guest access requires open access security, and is not compatible with WEP. • Guest users can be authenticated by way of an internal or external web landing page, or can be given open access to a restricted portion of the corporate network.

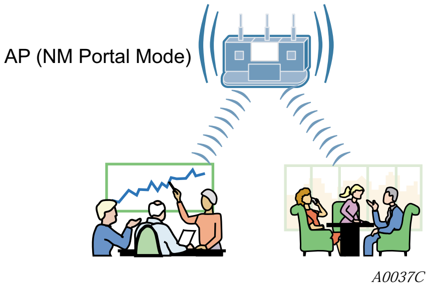
Example Deployment Scenarios

This section describes the feature decisions for an example company as a function of network size, management structure, and network services.

Example 1: Small office, single AP, possible future growth

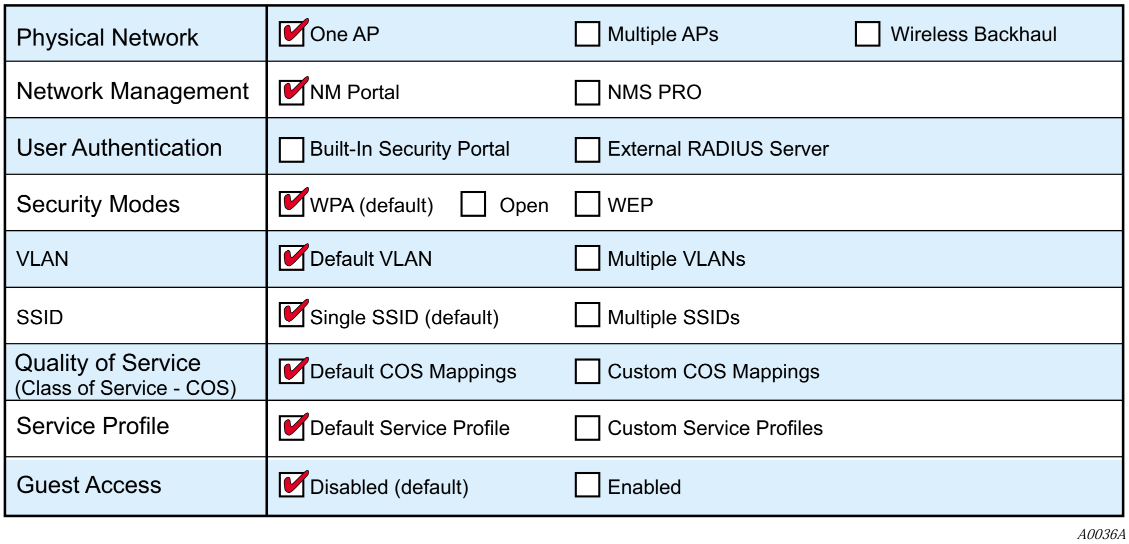
Acme Works begins as a small company with 20 users. The office is at a single location served by one access point connected to the wired backbone. The elements of the network are shown in Figure 5.

Figure 5: Example 1 Network



One AP is able to meet current coverage and capacity needs. The AP is configured as an NM Portal to assure that the appropriate network management structure will be in place in the event that the business expands and additional APs are required. Since the user base is small, there is no need for a RADIUS authentication infrastructure. The security mode is WPA with pre-shared keys (PSK) and AES encryption. A single SSID is in place, and the default VLAN, QoS, and service profiles are used.

Figure 6: Example 1 Feature Decisions



Physical Network	☑ One AP	□ Multiple APs	□ Wireless Backhaul
Network Management	☑ NM Portal	□ NMS PRO	
User Authentication	□ Built-In Security Portal	□ External RADIUS Server	
Security Modes	☑ WPA (default) □ Open	□ WEP	
VLAN	☑ Default VLAN	□ Multiple VLANs	
SSID	☑ Single SSID (default)	□ Multiple SSIDs	
Quality of Service (Class of Service - COS)	☑ Default COS Mappings	□ Custom COS Mappings	
Service Profile	☑ Default Service Profile	□ Custom Service Profiles	
Guest Access	☑ Disabled (default)	□ Enabled	

The following table lists the tasks required for configuration and provides pointers to the detailed instructions in this guide.

Table 3: Example 1 Configuration Tasks

Task	Process
Bring up the first (or only) 108 Mbps Wireless AP	**1** Make sure a DHCP server is available on the network, and create a DHCP reservation for the MAC address of this AP. **2** Have the information sheet shipped with the AP available. **3** Bootstrap the AP as an NM Portal. Defaults are acceptable for most settings. **4** Choose an SSID (wireless network name). **5** Choose an administrative password and WPA pre-shared key. **6** Configure clients with compatible WPA security using the same pre-shared key. References: “Initializing a Normal AP” on page 33, “Initializing the Portal AP” on page 36
Confirm that the network is up	• Open the IP Topology panel in NM Portal to confirm that the AP is listed as discovered. • Open the Station Management panel at any time to view a list of client stations associated to the AP. References: “Viewing IP Topology” on page 171 and “Managing Client Stations” on page 87.

Example 2: Small to mid-size business with wireless backhaul

Acme Works has now grown to 70 users. The site is the same as in Example 1; however Acme wants to provide coverage to a temporary building that has no wired connection. An additional AP is added to provide user access via a wireless backhaul (Figure 7).

Figure 7: Example 2 Network

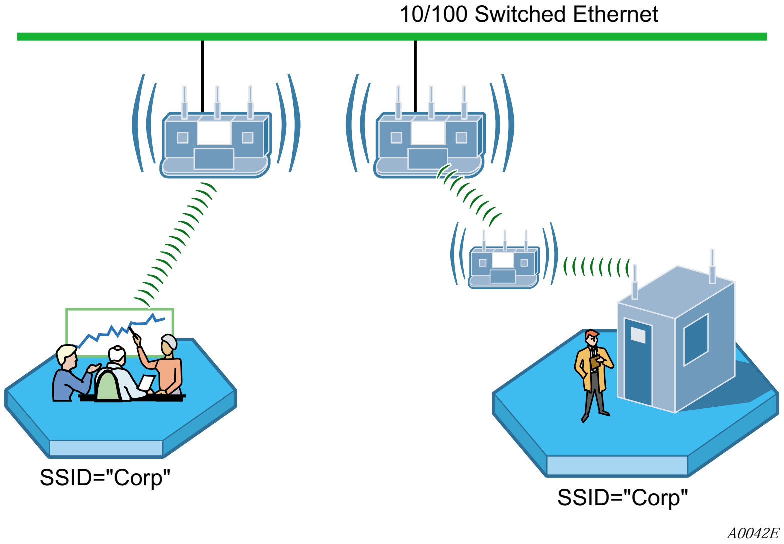
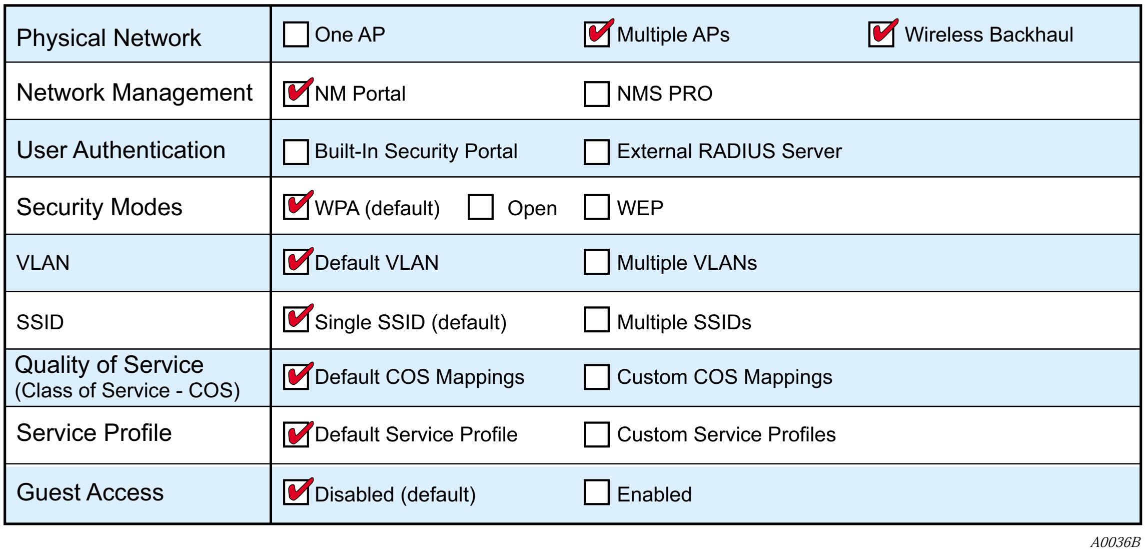


Figure 8 summarizes the feature decisions for this example. The security portal capability within NM Portal provides authentication for the backhaul AP. The security mode is WPA with pre-shared keys (PSK). A single SSID is in place, and the default VLAN, QoS, and service profiles are used.

Figure 8: Example 2 Feature Decisions



Physical Network	☐ One AP	☑ Multiple APs	☑ Wireless Backhaul
Network Management	☑ NM Portal	☐ NMS PRO	
User Authentication	☐ Built-In Security Portal	☐ External RADIUS Server	
Security Modes	☑ WPA (default) ☐ Open	☐ WEP	
VLAN	☑ Default VLAN	☐ Multiple VLANs	
SSID	☑ Single SSID (default)	☐ Multiple SSIDs	
Quality of Service (Class of Service - COS)	☑ Default COS Mappings	☐ Custom COS Mappings	
Service Profile	☑ Default Service Profile	☐ Custom Service Profiles	
Guest Access	☑ Disabled (default)	☐ Enabled	

A0036B

Example 3: Mid-size business, multiple SSIDs, multiple VLANs

Now a successful business, the management at Acme Works wants to position the company for continued growth. The company decides to deploy an external RADIUS server to manage user authentication centrally for the entire company. The RADIUS authentication infrastructure works well for a changing user population (employees joining, leaving, or moving to new departments) and readily supports further network service enhancements.

The company creates two SSIDs as a way to separate the Finance department network traffic from the main corporate network traffic. Two RADIUS servers are configured, each in its own authentication zone. To separate Finance department traffic from the overall network traffic, a Finance VLAN is created. A Finance service profile is also created and bound to the Finance SSID. The service profile is configured to include the Finance VLAN, high security and higher-than-normal COS. Once this structure is in place and a member of the Finance group is authenticated by way of the RADIUS server, the Finance group tag is passed to the 108 Mbps Wireless AP, and the Finance service profile is applied to the user.

The network configuration for this example is shown in Figure 9, and the feature decisions are shown in Figure 10.

Figure 9: Example 3 Network

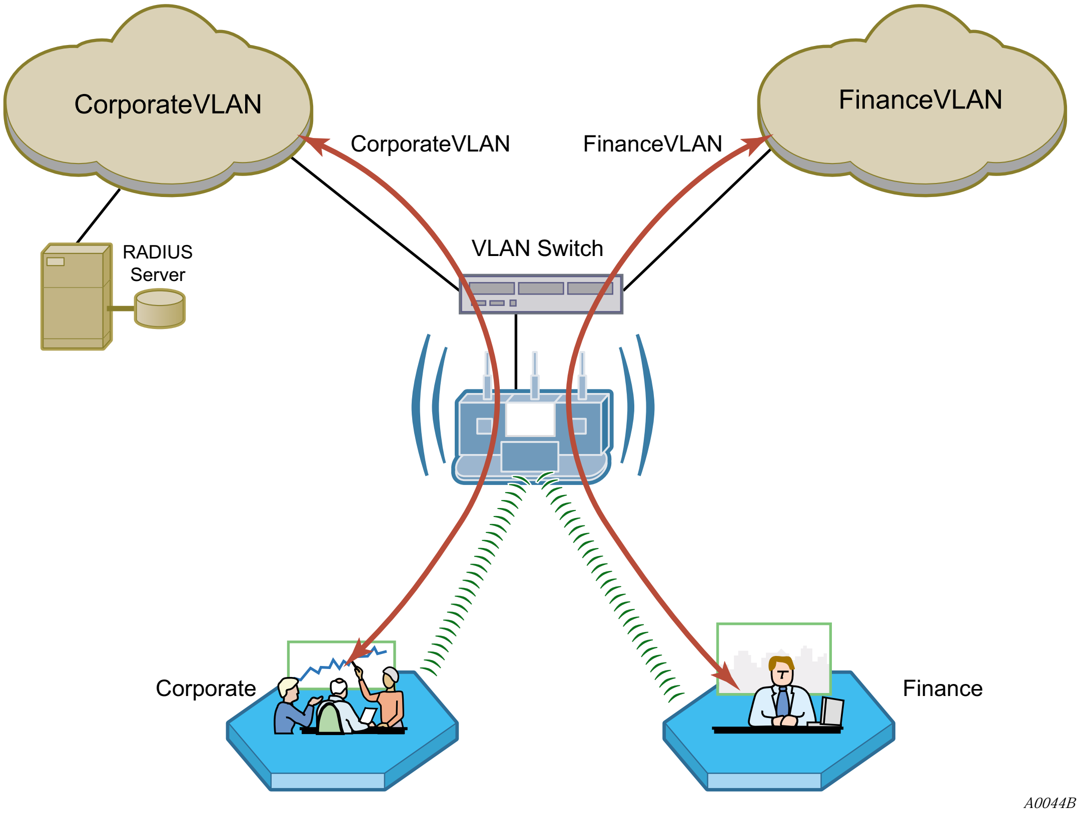
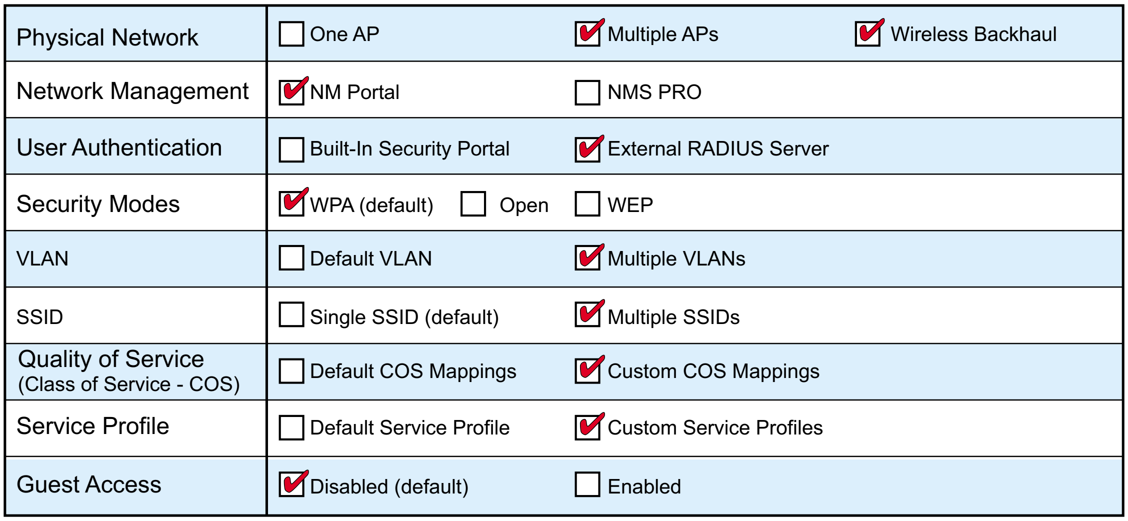


Figure 10: Example 3 Feature Decisions



Physical Network	□ One AP	☑ Multiple APs	☑ Wireless Backhaul
Network Management	☑ NM Portal	□ NMS PRO	
User Authentication	□ Built-In Security Portal	☑ External RADIUS Server	
Security Modes	☑ WPA (default) □ Open	□ WEP	
VLAN	□ Default VLAN	☑ Multiple VLANs	
SSID	□ Single SSID (default)	☑ Multiple SSIDs	
Quality of Service (Class of Service - COS)	□ Default COS Mappings	☑ Custom COS Mappings	
Service Profile	□ Default Service Profile	☑ Custom Service Profiles	
Guest Access	☑ Disabled (default)	□ Enabled	

A0036A

The following table lists the tasks required to link to an external RADIUS server and add multiple VLANs, and provides pointers to the detailed instructions in this guide.

Table 4: Example 3 Configuration Tasks

Task	Explanation
Add authentication servers and zones	**1** Identify the RADIUS server for each authentication zone. **2** Select the authentication option for the SSID, with reference to the defined authentication zone. References: “Configuring SSID Parameters” on page 79 and “Configuring Authentication Zones” on page 145
Set up VLANs	**1** Choose the VLAN structure for the network. **2** Configure the VLANs. Reference: “Configuring VLANs” on page 107.
Add VLANs to the service profiles	**1** Define or modify service profiles to include VLAN selection. **2** Bind each profile to an SSID with an existing or new user group. Reference: “Profile Table” on page 85 and “SSID Details” on page 83.

Example 4: Large business, guest access, extended network services

Acme Works is now a widely known and successful enterprise. With an ever increasing number of visitors requiring network access, the network administrator decides to implement a corporate guest access solution.

A guest VLAN and service profile are created and bound to the Corporate SSID, and a guest password is created. Guests can now visit Acme Works, log in using the guest password through a web browser, and obtain access to the resources available on the guest VLAN.

As additional needs arise, the network administrator can easily add new VLANs and service profiles, and change the available levels of service. New VLANs are created to segregate traffic for the Manufacturing and Engineering departments, and new service profiles are created to accommodate members of those departments. Special classes of service are assigned for applications sensitive to interruption or bandwidth fluctuation, such as voice over IP, and low priority, bandwidth-intensive applications such as FTP transfers.

The network configuration for this example is shown in Figure 11, and the feature decisions are shown in Figure 12.

Figure 11: Example 4 Network

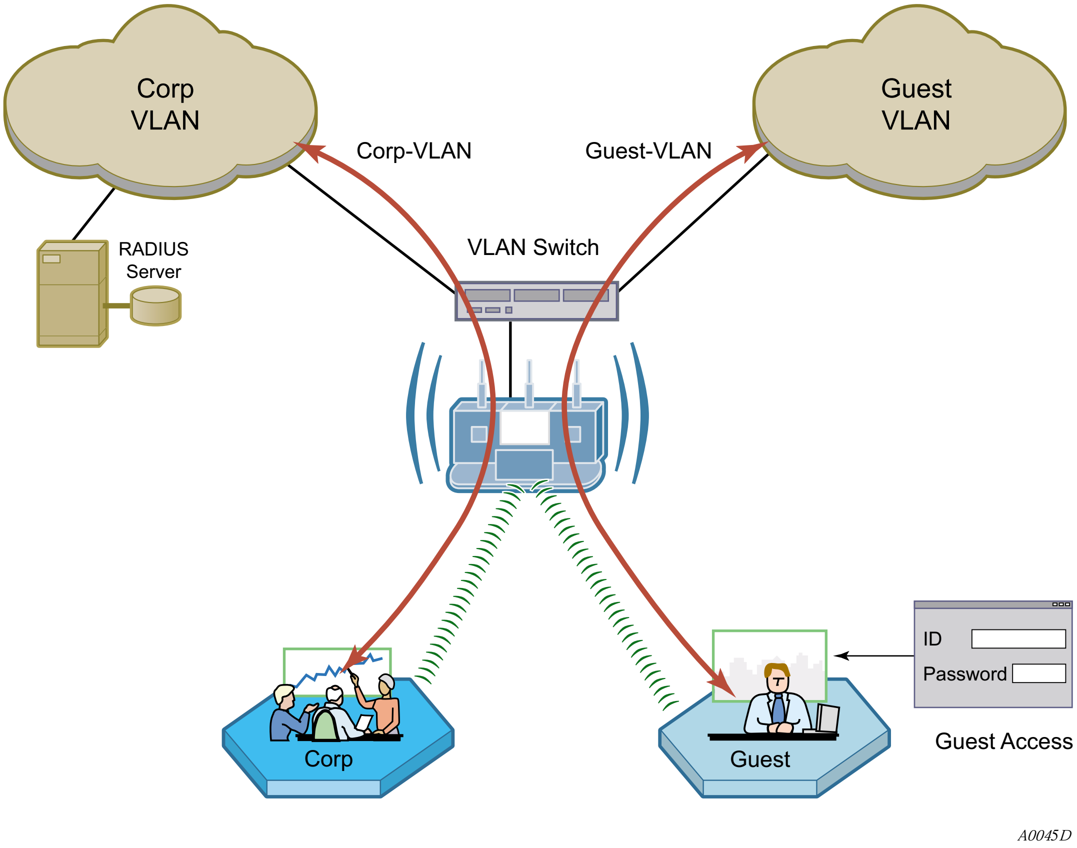
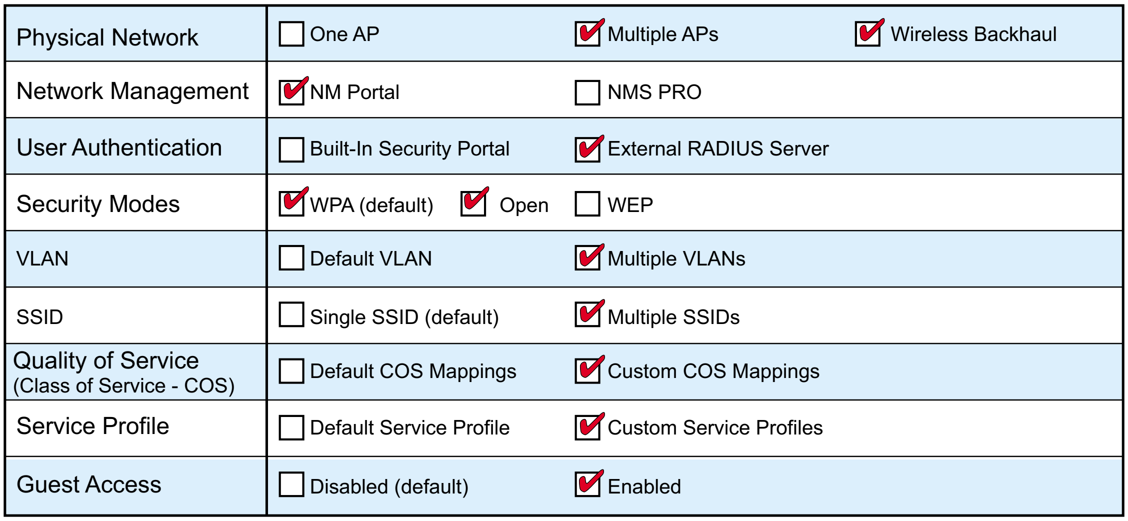


Figure 12: Example 4 Feature Decisions



Physical Network	☐ One AP	☑ Multiple APs	☑ Wireless Backhaul
Network Management	☑ NM Portal	☐ NMS PRO	
User Authentication	☐ Built-In Security Portal	☑ External RADIUS Server	
Security Modes	☑ WPA (default)	☑ Open	☐ WEP
VLAN	☐ Default VLAN	☑ Multiple VLANs	
SSID	☐ Single SSID (default)	☑ Multiple SSIDs	
Quality of Service (Class of Service - COS)	☐ Default COS Mappings	☑ Custom COS Mappings	
Service Profile	☐ Default Service Profile	☑ Custom Service Profiles	
Guest Access	☐ Disabled (default)	☑ Enabled	

A0036A

The following table lists the tasks required to configure guest access and provides pointers to the detailed instructions in this guide.

Table 5: Example 4 Configuration Tasks

Task	Explanation
Set up guest VLANs	• Configure a VLAN for guest access. Reference: “Configuring VLANs” on page 107.
Create guest service profile	• Add a guest service profile with the guest VLAN and desired COS and open security. Reference: “Profile Table” on page 85 and “SSID Details” on page 83.
Configure landing page	**1** Choose an internal or external landing page. **2** Assign guest password. Reference: “Configuring Guest Access” on page 158

Example 5: Large Campus with Branch Offices

With continued growth, the original Acme Works building is now surrounded by multiple buildings within a large campus setting. The company also has two branch offices in neighboring communities. The decision is made to implement Wireless LAN Network Management Software for enterprise-class network management. This solution will provide network administrators with extensive control and oversight, centralized monitoring, and fault management.

The campus buildings and branch offices lend themselves to a hierarchical management structure in which an NM Portal AP is configured in each building. Each NM Portal AP handles policy distribution and software upgrades at its location as directed by Wireless LAN Network Management Software. The NM Portal AP also serves as a backup security portal in the event that another RADIUS authentication server in its zone becomes unavailable.

The network configuration for this example is shown in Figure 13, and the feature decisions are shown in Figure 14.

Figure 13: Example 5 Network

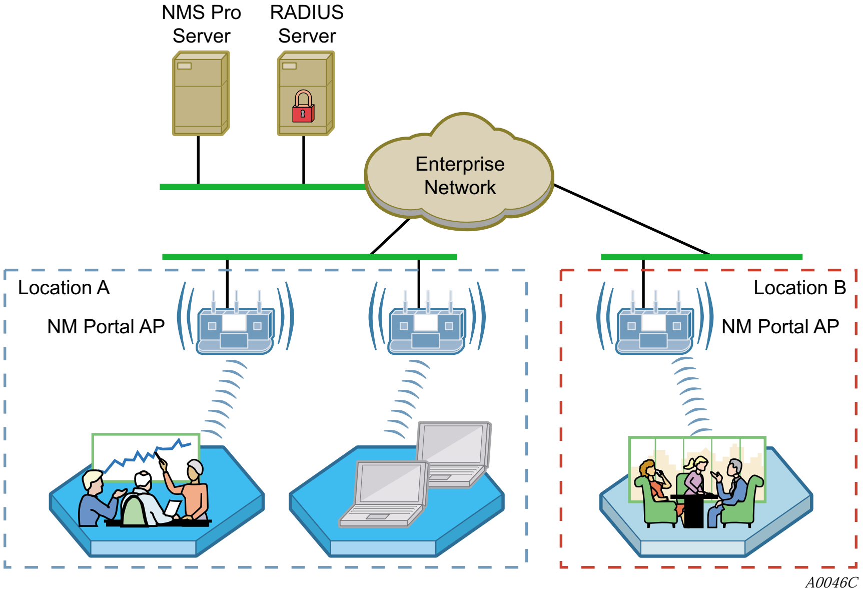
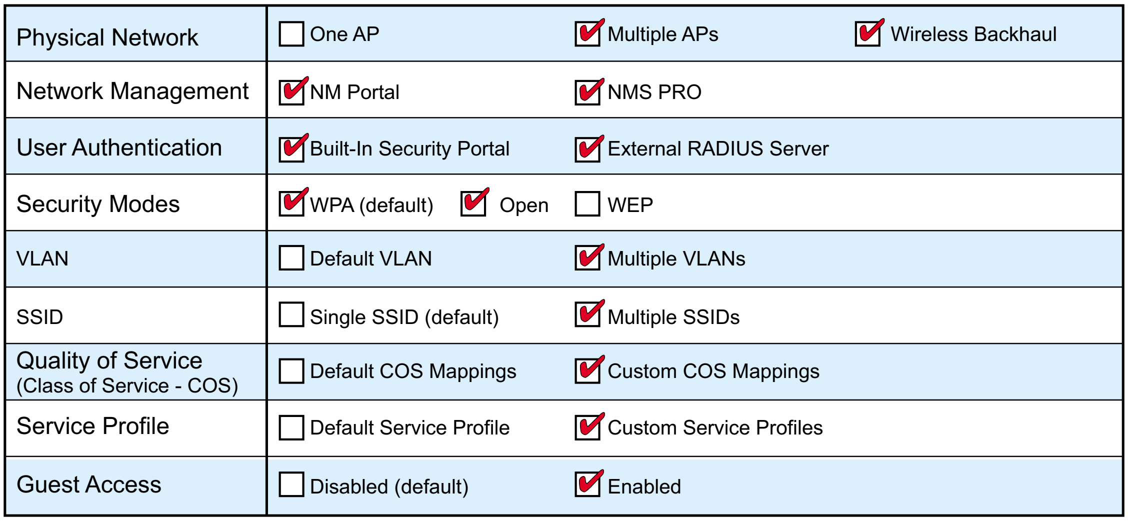


Figure 14: Example 5 Feature Decisions



Physical Network	□ One AP	☑ Multiple APs	☑ Wireless Backhaul
Network Management	☑ NM Portal	☑ NMS PRO	
User Authentication	☑ Built-In Security Portal	☑ External RADIUS Server	
Security Modes	☑ WPA (default) ☑ Open	□ WEP	
VLAN	□ Default VLAN	☑ Multiple VLANs	
SSID	□ Single SSID (default)	☑ Multiple SSIDs	
Quality of Service (Class of Service - COS)	□ Default COS Mappings	☑ Custom COS Mappings	
Service Profile	□ Default Service Profile	☑ Custom Service Profiles	
Guest Access	□ Disabled (default)	☑ Enabled	

A0036A

The following table summarizes the tasks required to provide network management for the campus installation:

Table 6: Example 5 Configuration Tasks

Task	Explanation
Install Wireless LAN Network Management Software	Reference: *Wireless LAN Network Management Software Installation and Configuration Guide*
Enroll APs	• Use the NM Portal in the local building or the campus Wireless LAN Network Management Software system to enroll additional APs. Reference: "Enrolling APs" on page 167 or the *Wireless LAN Network Management Software Installation and Configuration Guide*
Create and distribute policies	• Use Wireless LAN Network Management Software to create configuration policies and distribute them to APs across the network. Reference: *Wireless LAN Network Management Software Installation and Configuration Guide*

3 Installing the Access Point Using the Configuration Interfaces

This chapter explains how to install and quickly configure the 108 Mbps Wireless Access Point and provides instructions for accessing the web and command line interfaces. The chapter includes the following topics:

- **Hardware Components**
- **System Requirements**
- **Installation Requirements**
- **Installing the Access Point**
- **Using the Configuration Interfaces**
- **Using AP Quick Start to Initialize the Access Point**
- **Navigating the Web Interface**
- **Configuration Wizards**

Hardware Components

The 108 Mbps Wireless Access Point shipping package contains the following items:

- 108 Mbps Wireless Access Point
- Power supply and separate AC cord
- Software and documentation

System Requirements

The following are required to connect to the 108 Mbps Wireless Access Point:

- For web browser or network management portal access, a computer with a web browser capable of secure HTTP connections (HTTPS)
- For SSH connection, a computer with an SSH utility (the PuTTY application meets this requirement and is available as freeware)
- 10/100 Ethernet cable to connect to the AP

The computer designated for AP access should be located on the same Local Area Network (LAN), with a compatible IP address and subnet mask, or it must be able to be routed to the AP.

To connect directly to the console port in order to access the command line interface, have the following available:

- A 9-pin DCE female to female null modem connector to connect the PC to the Access Point
- Terminal emulator software

Installation Requirements

108 Mbps Wireless Access Points are radio frequency devices and are therefore susceptible to RF interference and obstructions. When selecting locations for AP placement, try to choose places that

are free of large metallic structures such as equipment racks, steel bookcases or filing cabinets, or crowded by computer enclosures.

If using an external antenna with the AP (optional), try to place the unit as high as possible, where it is free of obstruction. Install the AP away from sources of RF interference, such as microwave ovens, cordless phones, electric motors, and similar appliances.

Power and Cabling Requirements

The following equipment is required to install the 108 Mbps Wireless Access Point:

- AC power outlet (100-240V, 50-60Hz standard) to power the AP (a surge-protected power supply is recommended)
- RJ-45 port on a standard 10/100BaseT Ethernet device (hub, switch, router, or similar device), if connecting to a wired network
- Industry standard Category 5 UTP Ethernet cables
- 9-pin-to-9-pin DCE serial null modem cable or serial to USB cable, if connecting the console

Network Information Requirements

Have the following information accessible before configuring the AP:

- IP address assigned to the AP (fixed IP address or DHCP-reserved address)
- IP addresses for the default gateway, DNS Server and NTP Server, if DHCP is not used to provide IP addresses
- IP address of the SMTP email server, if the AP is to send alerts to a specified email address
- Email address of the administrator who will receive the alerts

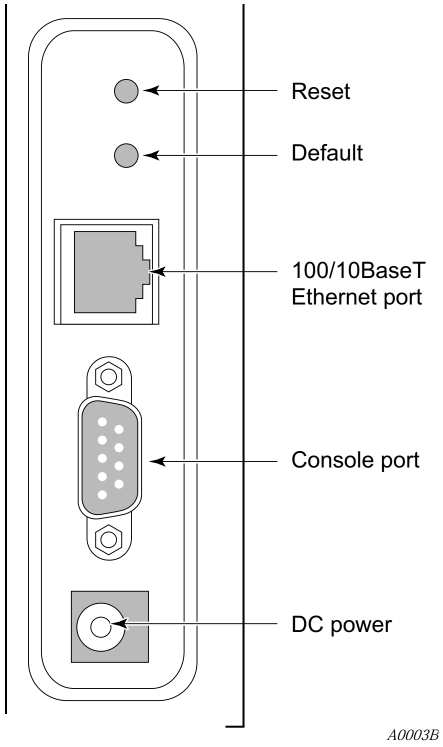
Installing the Access Point

Follow these steps to install the 108 Mbps Wireless Access Point:

1. Connect the Ethernet cable to the RJ-45 Ethernet connector on the AP (see Figure 15).
2. Plug the other end of the Ethernet cable into an available Ethernet port on your wired network.
3. (Optional) If an external antenna is to be used, attach it to the AP. Place or mount the antenna in an unobstructed location.
4. Plug the AC power cable into the power module.
5. Plug the other end of the AC power cable into an approved three-prong grounded outlet (surge-protected and/or UPS is recommended).
6. Connect the power module connector to the power connector on the AP.

The 108 Mbps Wireless Access Point powers up automatically.

Figure 15: 108 Mbps Wireless AP Connections



Using Power Over Ethernet

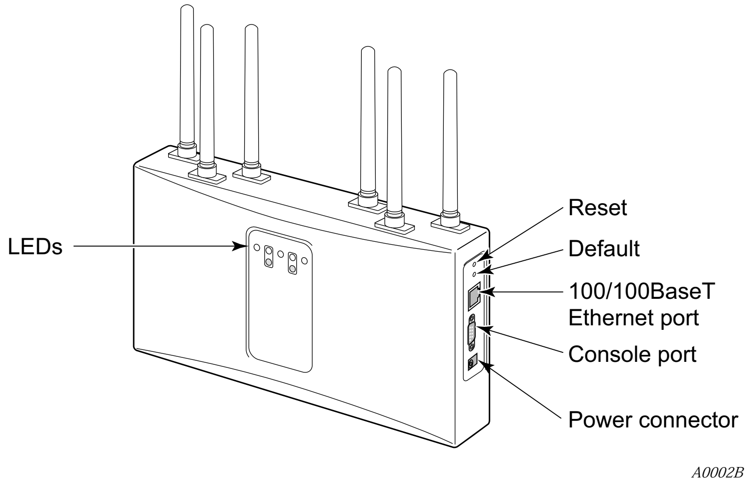
Power-over-Ethernet, based on the 802.3af standard, can be used to supply power to the 108 Mbps Wireless AP. If both DC power and power-over-Ethernet are used at the same time, then failover takes place automatically in the event that one of the power sources is lost. For failover, the following rules apply:

- The AP uses the power source with the highest voltage.
- Unplugging either cable causes power to switch automatically to the other source.

Placement and Orientation

Make sure that the 108 Mbps Wireless AP is positioned in an upright position for airflow and antenna placement (Figure 16).

Figure 16: 108 Mbps Wireless AP Placement



Verifying the Installation

To verify the 108 Mbps Wireless Access Point is operational, examine the front of the AP.

- Is the status LED red or green? If not, check the power connections and whether or not the AC outlet has power.
- (For wired-AP installations) Is the Ethernet connection LED on? If not, check the Ethernet cable to make sure it is seated securely in both the AP and the network port.

Interpreting the LEDs

Refer to Figure 17 and Table 7 for LED definition.

Figure 17: 108 Mbps Wireless AP LEDs

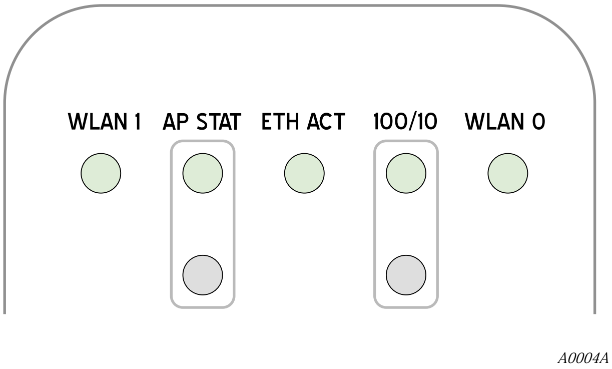


Table 7: LED Definitions

LED	Description
WLAN1	Blinks green for activity.
AP STAT	There are two AP status LEDs that indicate the AP status. When the AP is reset or powered on, the bottom LED turns red and then the top LED blinks green. Once the AP successfully boots up, the top LED turns green and stays green. When the AP is reset to defaults, the LEDs light up in the same sequence as described above. If the AP has a buzzer installed, two short beeps indicate that the AP is being reset to defaults.
ETH ACT	Blinks green for activity.
100/10	Indicates Ethernet Link. Two LEDs. Only one of them will be lit up at a time. • Top LED: 100BT Link – Lights up Green when 100 Mbit link is established. Off means no link on 100 Mbit. • Bottom LED: 10BT Link – Lights up Yellow when 10 Mbit link is established. Off means no link on 10 Mbit.
WLAN0	Blinks green for activity.

Connecting the Serial Port

Follow these steps to connect a terminal to the serial port for command line interface access:

1. Attach a serial null modem cable to the AP (see Figure 15).
2. Attach the other end of the cable to the serial port of your computer.
3. Use a terminal emulation tool such as HyperTerminal. Configure the terminal as follows:
   - 115,200 BAUD
   - 8-bits
   - No parity
   - 1 stop bit
   - No flow control

A command prompt should now be available to access the command line interface.

Resetting the Access Point

Reset the AP in any of the following ways. If the AP has a buzzer installed, the AP beeps once when reset. If the AP has a buzzer installed and is reset to factory defaults, then the AP beeps twice when booted.

Method	Description
Web browser interface	Use the Configuration Management panel under System Configuration. See “Reset Configuration” on page 219.
Reset button	Press the reset button on the side of the AP.
Power down	Power down the AP by disconnecting the power cable (not recommended).

Reset the configuration of the AP to the factory default in any of the following ways:

Method	Description
Web browser interface	Use the Configuration Management panel under System Configuration. See "Reset Configuration" on page 219.

CLI	Use the command sequence
	`config`
	`system >`
	`reset-to-defaults factory-defaults`

Reset buttons on the AP	This is useful if the administrative password is lost; however, before performing the reset, make sure to have the original factory-assigned AP password available. Follow these steps: **1** Make sure the AP is connected to power (power adaptor or Power-over-Ethernet). **2** On the side of the AP, hold down both the Reset and the Default buttons. The button closest to the antenna is the Reset button. The button below it is the Default button. **3** Release only the Reset button and continue to hold down the Default button. After 10 seconds, the Status LED blinks from Red to Green twice. If the AP has a buzzer, a beep indicates that the restore operation has started. **4** Now release the Default button. The AP continues to reboot.The Status LED turns Green when the reboot is successful and the AP is operational. During this process, all passwords and configurations are reset to factory defaults. If the AP was previously enrolled in a network, it must be re-enrolled. The new administrator password is now the original AP unique password that was set at the factory.

Using the Configuration Interfaces

Four different secure interfaces are available for administering the 108 Mbps Wireless Access Point:

- Web browser (https)
- Command line interface (SSH or console)
- SNMP (SNMPv3)
- Policy management (https, XML-based)

This section explains how to access each of these interfaces. The configuration procedures in this guide are all presented using the web browser interface. For additional information on the CLI, see the *CLI Reference Manual*.

Using the Web Browser Interface

The 108 Mbps Wireless AP web browser interface is the easiest way to configure an AP or check the current settings. It includes the QuickStart facility to get the AP running as quickly as possible and full set of AP features. NM Portal can also be launched from the web interface.

NOTE: In the web interface, a red asterisk (*) next to a field name indicates that the field is required. Error messages are presented in text near the top of the panel.

To connect to the AP using the web browser interface requires an IP connection to the AP network and a computer with a browser capable of Secure Sockets Layer (SSL) connections. Follow these steps:

1 Launch the web browser.

- **a** If your network has a DHCP server, enter the DHCP-assigned address of the AP in the address bar.
- **b** If your network does not use a DHCP server, assign the static address 192.168.1.1/24 to your computer, and then enter `https://192.168.1.254` in the browser address bar.

i **NOTE:** Each AP has DHCP enabled by default. If you are installing the AP on a network that already has a DHCP server, enter the DHCP-assigned address of the AP to access the web interface.

2 Depending on the browser security settings, a security alert may open with a prompt on whether to accept the PLANEX security certificate. Click **Yes** to accept the certificate and to open the login panel.

3 In the login panel, enter or confirm the administrative user name, enter the password, select a language, and click **OK** to open the web interface. The factory default for administrator access is user name: `admin`. If the AP has not been initialized, the user name field is grayed out. The factory default password is shipped with the AP on a paper insert. Use the password from the insert to log in.

4 The system response at this point depends upon whether the AP has already been initialized.

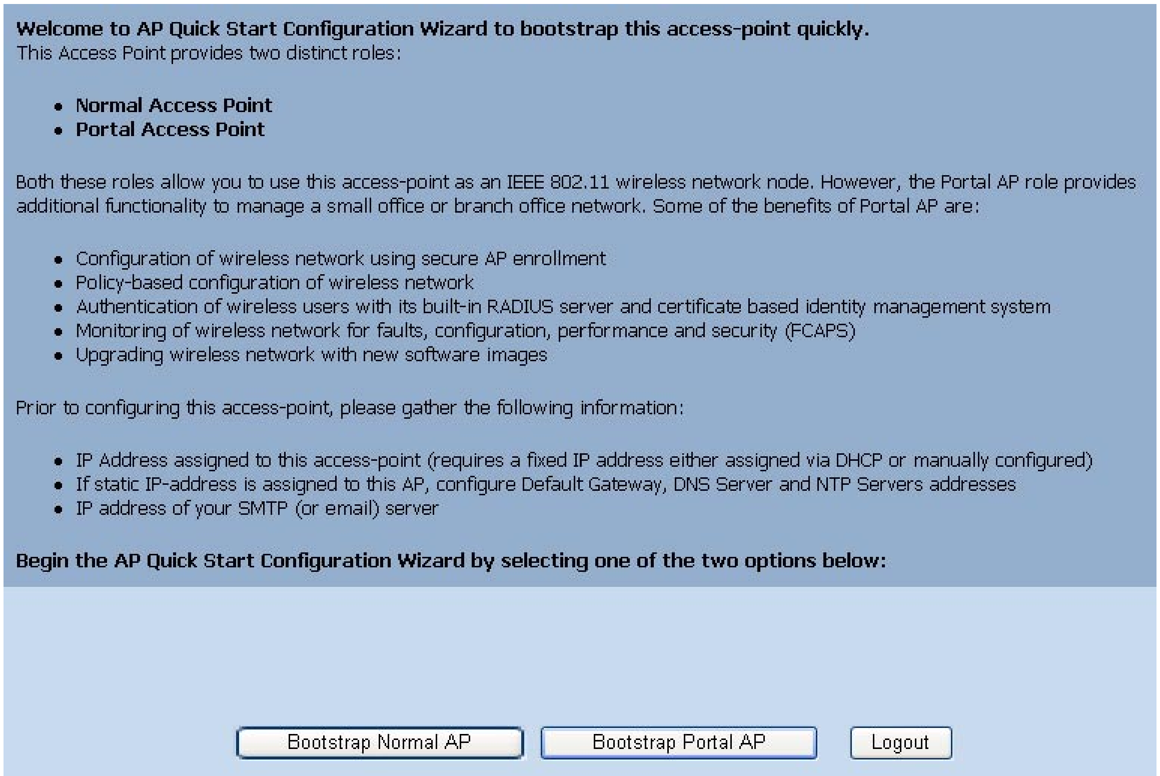
- **a** If the AP has been initialized, the Home feature panel opens. See “The Home Panel” on page 37.
- **b** If the AP has not been initialized, the QuickStart Welcome panel opens. Use the QuickStart panels, described in the next section, to quickly configure the AP.

Using AP Quick Start to Initialize the Access Point

When accessing the web interface for the first time or after resetting the AP to factory defaults, the Welcome panel of the AP Quick Start Wizard opens (Figure 18). From this panel, initialize the AP in either of two roles:

- Normal Access Point
- Portal Access Point (NM Portal)

Figure 18: AP Quick Start Welcome Panel



Welcome to AP Quick Start Configuration Wizard to bootstrap this access-point quickly.
This Access Point provides two distinct roles:

- **Normal Access Point**
- **Portal Access Point**

Both these roles allow you to use this access-point as an IEEE 802.11 wireless network node. However, the Portal AP role provides additional functionality to manage a small office or branch office network. Some of the benefits of Portal AP are:

- Configuration of wireless network using secure AP enrollment
- Policy-based configuration of wireless network
- Authentication of wireless users with its built-in RADIUS server and certificate based identity management system
- Monitoring of wireless network for faults, configuration, performance and security (FCAPS)
- Upgrading wireless network with new software images

Prior to configuring this access-point, please gather the following information:

- IP Address assigned to this access-point (requires a fixed IP address either assigned via DHCP or manually configured)
- If static IP-address is assigned to this AP, configure Default Gateway, DNS Server and NTP Servers addresses
- IP address of your SMTP (or email) server

Begin the AP Quick Start Configuration Wizard by selecting one of the two options below:

Both roles allow the AP to function as an IEEE 802.11 wireless network node. As a portal AP, the following additional functions are available:

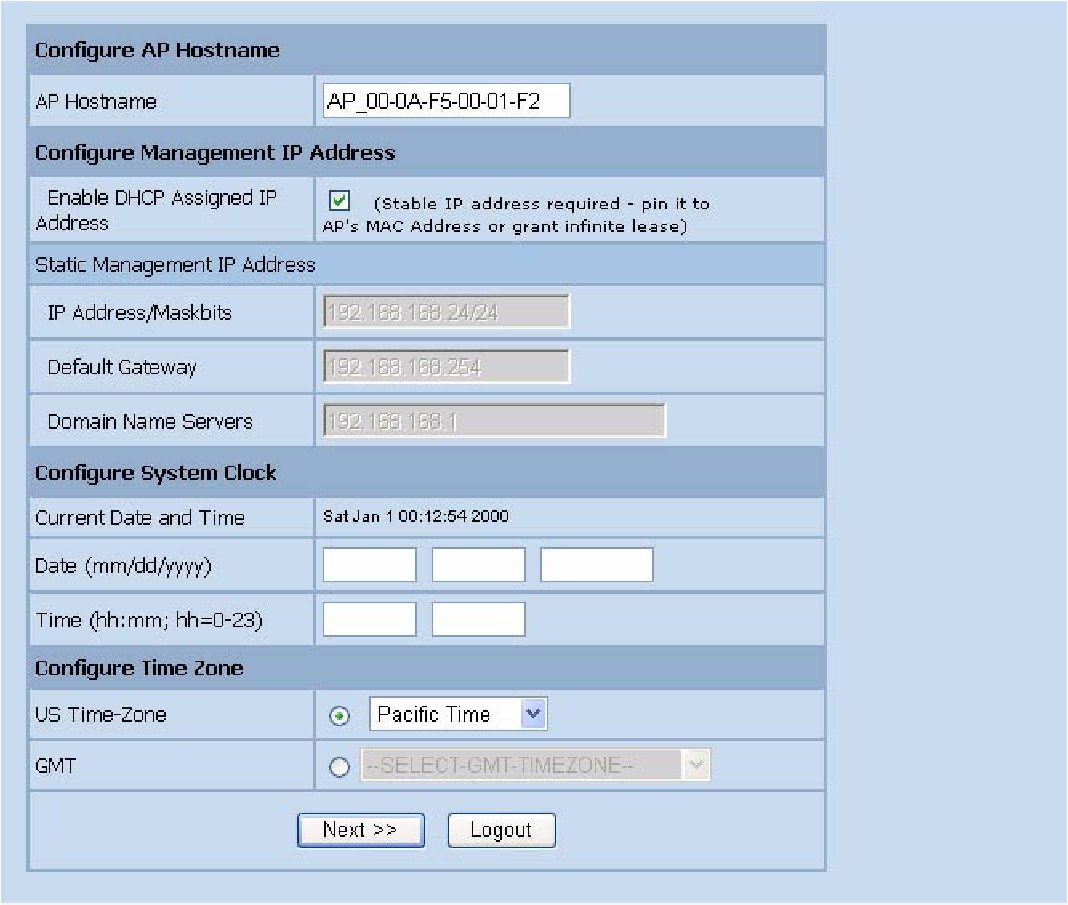
- Configuration of the PLANEX wireless network using secure AP enrollment and policy-based configuration of APs
- Authentication of wireless users via built-in RADIUS server and certificate based identity management system
- Monitoring of PLANEX network for faults, configuration alerts, performance and security (FCAPS)
- Upgrade of the 108 Mbps Wireless AP network with new software images

Initializing a Normal AP

1 Click **Bootstrap Normal AP** from the Quick Start Welcome panel to open the first initialization panel (Figure 19).

NOTE: Click **Logout** if it is necessary to leave the Quick Start panels. If you log out prior to completing the set-up process, then settings are not saved.

Figure 19: QuickStart Configuration Parameters



Configure AP Hostname	
AP Hostname	AP_00-0A-F5-00-01-F2
Configure Management IP Address	
Enable DHCP Assigned IP Address	☑ (Stable IP address required - pin it to AP's MAC Address or grant infinite lease)
Static Management IP Address	
IP Address/Maskbits	192.168.168.24/24
Default Gateway	192.168.168.254
Domain Name Servers	192.168.168.1
Configure System Clock	
Current Date and Time	Sat Jan 1 00:12:54 2000
Date (mm/dd/yyyy)	
Time (hh:mm; hh=0-23)	
Configure Time Zone	
US Time-Zone	● Pacific Time
GMT	○ --SELECT-GMT-TIMEZONE--

The following fields are available on this panel; however, none is required to get the AP up and running:

Field — **Description**

AP Hostname — Alphanumeric name for the AP. The factory default for this field is AP followed by the MAC address of the AP's Ethernet interface (eth0).

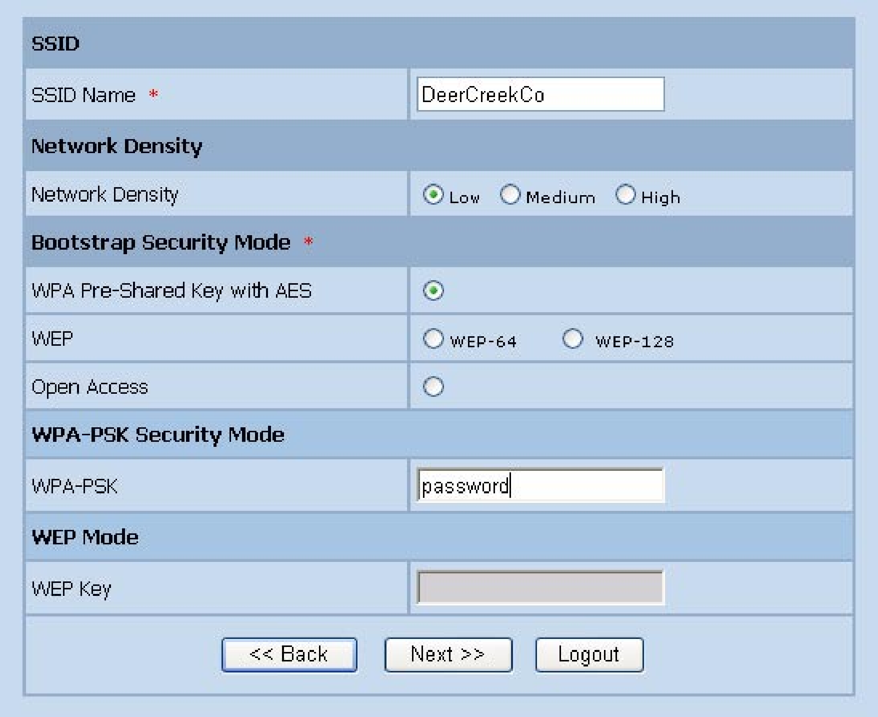
Enable DHCP Assigned IP Address — Checkbox that indicates whether DHCP is used to obtain an IP address. If the box is cleared, the static Management IP Address fields are activated; if the box is selected, the static Management IP Address fields are inactive.

IP Address/Maskbits — Static IP address and subnet prefix for the AP. Required if the IP address is not obtained automatically. The default is `192.168.1.254/24.`

Field	Description
Default Gateway	IP address of the gateway to the wired network. Required if the IP address is not obtained automatically to provide complete network access. The default is the existing network gateway.
Domain Name Servers	IP address of the server supplying DNS service. Required if the IP address is not obtained automatically to provide complete network access. The default is the DNS server for the existing network.
Date	Current date in MM/DD/YYYY format
Time	Current time in HH:MM:SS format (hours 0-23)
Time Zone	US-zone or GMT option. For US zone, click the radio button and select a time zone. For GMT, click the radio button and select an offset in HH:MM format.

2 Click **Next** to continue to the next panel (Figure 20). Use this panel to configure network identity.

Figure 20: QuickStart Network Identity



SSID	
SSID Name *	DeerCreekCo
Network Density	
Network Density	● Low ○ Medium ○ High
Bootstrap Security Mode *	
WPA Pre-Shared Key with AES	●
WEP	○ WEP-64 ○ WEP-128
Open Access	○
WPA-PSK Security Mode	
WPA-PSK	password
WEP Mode	
WEP Key	

3 Configure the following information on this panel:

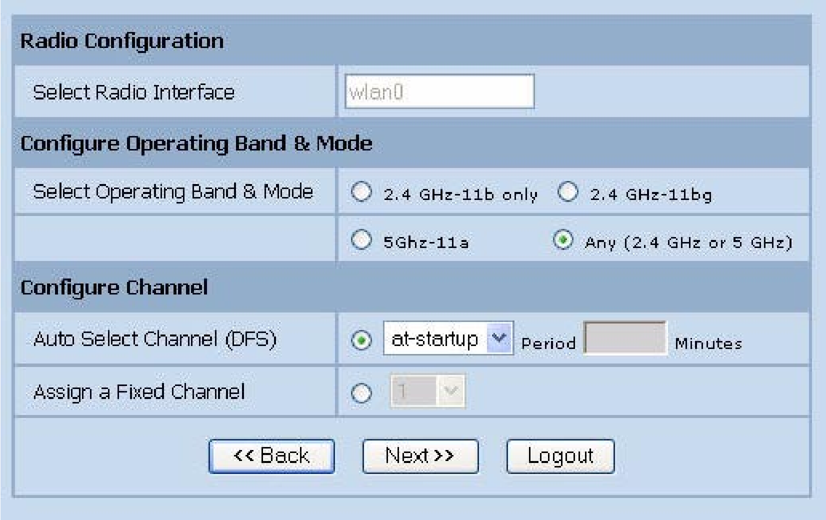
Field	Description
SSID Name	Service set identifier for the network, also known as the Wireless Network Name. The default name must be changed. (required)
Network Density	Indication of how close the APs will be to each other. For closely spaced APs that can support high data rates, select the high density option. For maximum coverage at lower data rates, selection the low density option. The default setting is Low.

Field	Description
Bootstrap Security Mode	WPA-PSK, WEP-64, WEP-128, or Open security option. The option determines the security mode for the AP.
WPA-PSK Security Mode	Activated if WPA is selected as the security mode. Enter a alphanumeric string at least eight characters in length. (required if security mode is WPA-PSK).
WEP Key	Activated if WEP is selected as the security mode. Enter a WEP key. A WEP-64 key is 10 hex characters, and a WEP-128 key is 26 hex characters. (required if security mode is WEP)

4 Click **Next** after making selections.

The last two panels (Figure 21) configure each of up to two radios on the AP. After entering settings on the first of the two panels, click **Next** to open the second panel.

Figure 21: QuickStart Radio Parameters



Radio Configuration

Select Radio Interface	wlan0

Configure Operating Band & Mode

Select Operating Band & Mode	○ 2.4 GHz-11b only ○ 2.4 GHz-11bg
	○ 5Ghz-11a ● Any (2.4 GHz or 5 GHz)

Configure Channel

Auto Select Channel (DFS)	● at-startup Period Minutes
Assign a Fixed Channel	○ 1

5 Set the following information:

Field	Description
Select Radio Interface	Specific radio to be configured on the AP (wlan0 or wlan1). These correspond to the WLAN0 and WLAN1 LEDs on the front of the AP.
Select Operating Band and Mode	802.11b mode in the 2.4-GHz band, 802.11b or g mode in the 2.4-GHz band, 802.11a mode in the 5-GHz band, or auto selection (Any).
Configure Channel	Select Auto-Select Channel or Assign Fixed Channel options: • Auto-Select: Select At Start-up to automatically determine the channel when the AP is booted, or Periodic to auto-select the channel at the specified number of minutes. • Assign Fixed Channel: Select a static channel. In both of these cases, the channel set used for auto-scanning can also be restricted.

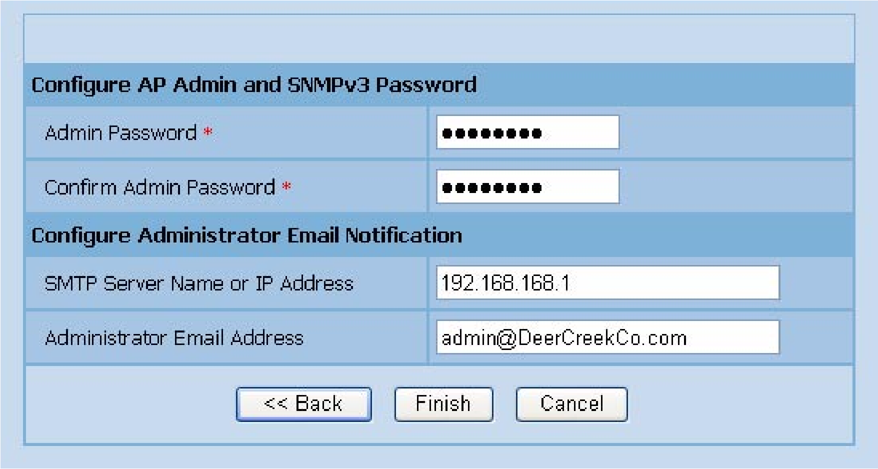
NOTE: The defaults for radio configuration have been selected for the best operational radio behavior across a variety of environments. Modifying these parameters alters radio behavior, which may have an impact on network performance or services. For example, selecting an operating band of 5GHz (802.11a) may prevent legacy client adapters from associating to the AP.

6 After entering settings for both radios, click **Finish** to complete the initialization process. (If initializing a portal AP, as described in the next section, the button is labeled **Next**.)

Initializing the Portal AP

Using the QuickStart panels to initialize NM Portal is similar to initializing a normal AP. The first four panels, as described in the previous section, are the same as for the normal AP. When configuring the second radio, click **Next** to set the administration and networking configuration (Figure 22).

Figure 22: Portal QuickStart panel



Configure AP Admin and SNMPv3 Password

Admin Password *	●●●●●●●●
Confirm Admin Password *	●●●●●●●●

Configure Administrator Email Notification

SMTP Server Name or IP Address	192.168.168.1
Administrator Email Address	admin@DeerCreekCo.com

7 Enter the following information consistent with your corporate standards:

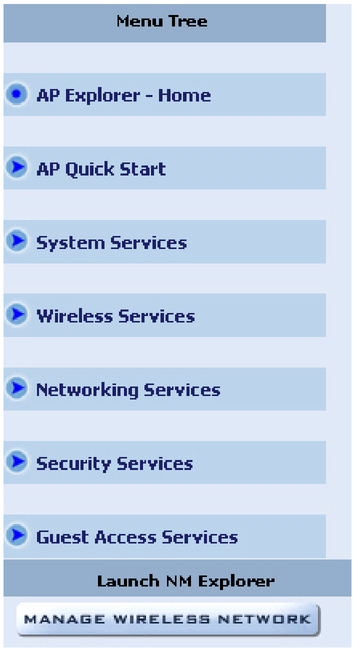
Field	Description
Admin Password	Enter and confirm the password used to manage this AP and other enrolled APs. The password must be between 8 and 32 characters and is used for local administrator login and SNMP v3 login. (required)
SMTP Server Name or IP Address	Address of your SMTP server
Administrator Email Address	Email address of the person to be notified regarding alerts

8 Click **Finish** to complete the initialization process and bring up the AP Explorer Home panel. The process takes approximately two minutes. When the process is complete, the Home panel opens.

Navigating the Web Interface

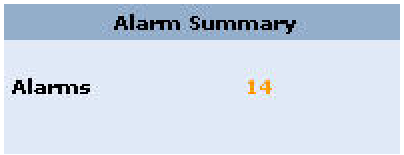
The 108 Mbps Wireless AP web interface is divided into three main areas. The menu tree (Figure 23) provides access to all the panels and features of the web interface. To expand a menu in the menu tree, click the arrow to the left of the menu name.

Figure 23: Menu Tree



The lower left alarm panel (Figure 24) lists the number of current alarms.To update the alarm summary, periodically click the browser refresh button.

Figure 24: Alarm Area



Alarm Summary

Alarms 14

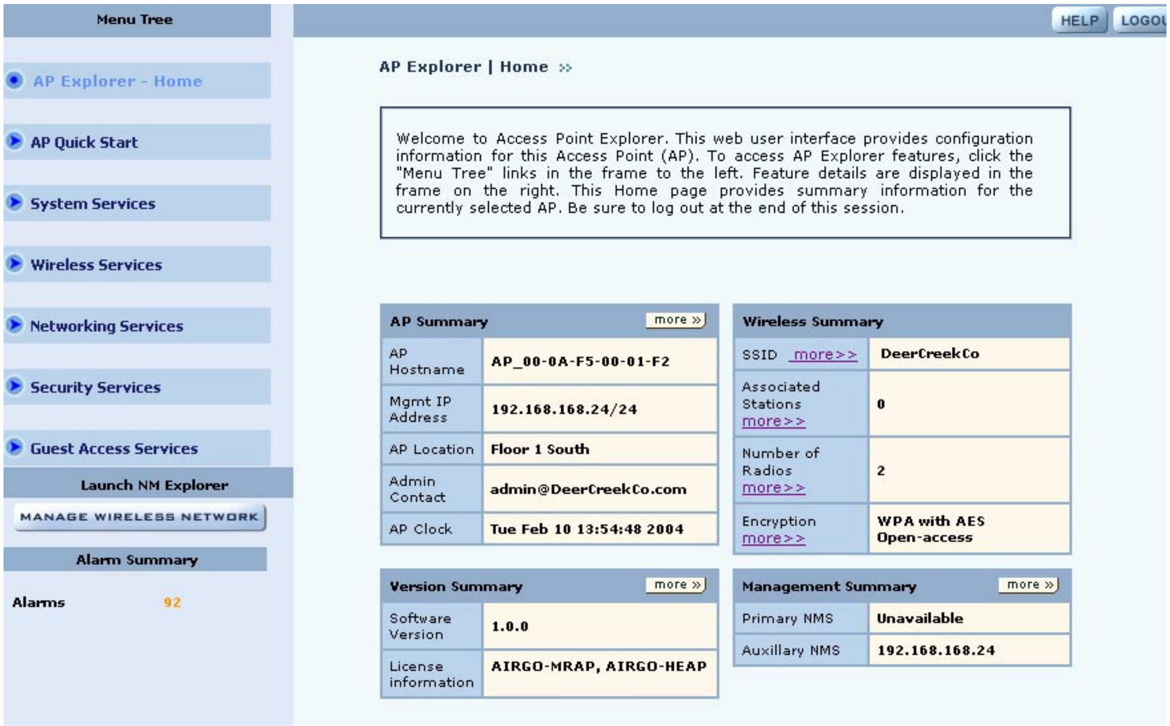
When you select an item from the menu tree, the information is displayed in the Detail panel, which takes up most of the browser window (shown for the Home panel in Figure 25).

The Home Panel

The Home panel (Figure 25) opens when you first log in to the web interface, or if **Home** is selected from the menu tree. The Home screen contains top-level summary information about the AP. To access detailed information, click **More** for any of the following sections:

- AP Summary—Opens the Bootstrap Configuration panel under the AP Quick Start menu (see “Quick Start Panels” on page 39).
- Version Summary—Opens a detailed list of model and serial numbers and hardware and software versions (see “Version Table” on page 44).
- Wireless Summary links—Opens panels to configure SSID, client stations, radios, and encryption.
- Management Summary—Shows current network management address settings.

Figure 25: Home Panel



Welcome to Access Point Explorer. This web user interface provides configuration information for this Access Point (AP). To access AP Explorer features, click the "Menu Tree" links in the frame to the left. Feature details are displayed in the frame on the right. This Home page provides summary information for the currently selected AP. Be sure to log out at the end of this session.

Alarm Summary	
Alarms	92

AP Summary	
AP Hostname	AP_00-0A-F5-00-01-F2
Mgmt IP Address	192.168.168.24/24
AP Location	Floor 1 South
Admin Contact	admin@DeerCreekCo.com
AP Clock	Tue Feb 10 13:54:48 2004

Wireless Summary	
SSID more>>	DeerCreekCo
Associated Stations more>>	0
Number of Radios more>>	2
Encryption more>>	WPA with AES Open-access

Version Summary	
Software Version	1.0.0
License information	AIRGO-MRAP, AIRGO-HEAP

Management Summary	
Primary NMS	Unavailable
Auxillary NMS	192.168.168.24

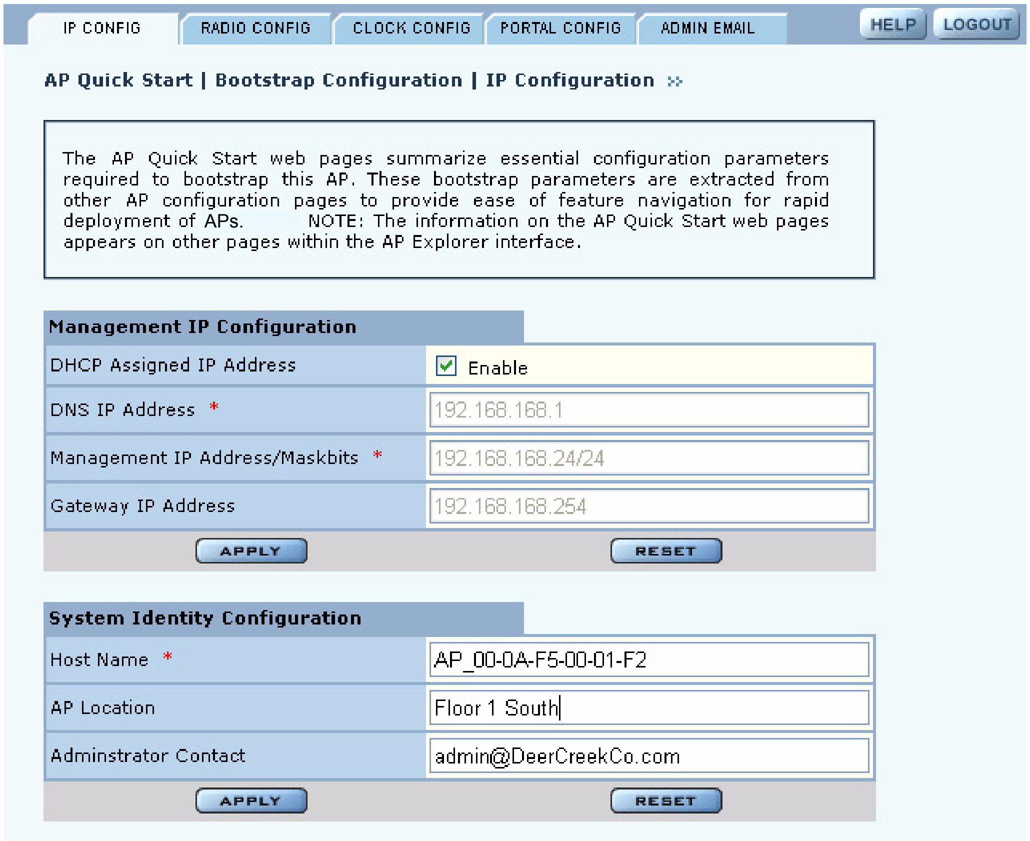
Quick Start Panels

Use the AP Quick Start menu items to open the Bootstrap Configuration and Version panels. Each of the tabs in the Bootstrap Configuration panel corresponds to one of the screens used to initialize an AP in AP Quick Start.

IP Config Tab

The IP Config tab opens when you choose Bootstrap Configuration is selected from the AP Quick Start menu (Figure 26). Use this tab to configure addresses for the bootstrap configuration.

Figure 26: AP Quick Start - Bootstrap Configuration - IP Config



AP Quick Start | Bootstrap Configuration | IP Configuration

The AP Quick Start web pages summarize essential configuration parameters required to bootstrap this AP. These bootstrap parameters are extracted from other AP configuration pages to provide ease of feature navigation for rapid deployment of APs. NOTE: The information on the AP Quick Start web pages appears on other pages within the AP Explorer interface.

Management IP Configuration

DHCP Assigned IP Address	☑ Enable
DNS IP Address *	192.168.168.1
Management IP Address/Maskbits *	192.168.168.24/24
Gateway IP Address	192.168.168.254

System Identity Configuration

Host Name *	AP_00-0A-F5-00-01-F2
AP Location	Floor 1 South
Adminstrator Contact	admin@DeerCreekCo.com

This tab contains the following settings:

Field	Description
DHCP Assigned IP Address	Indicate whether to use DHCP to obtain an IP address for the AP. If the box is cleared, the other Management IP Configuration fields are activated; if the box is selected, the other Management IP Configuration fields are inactive.

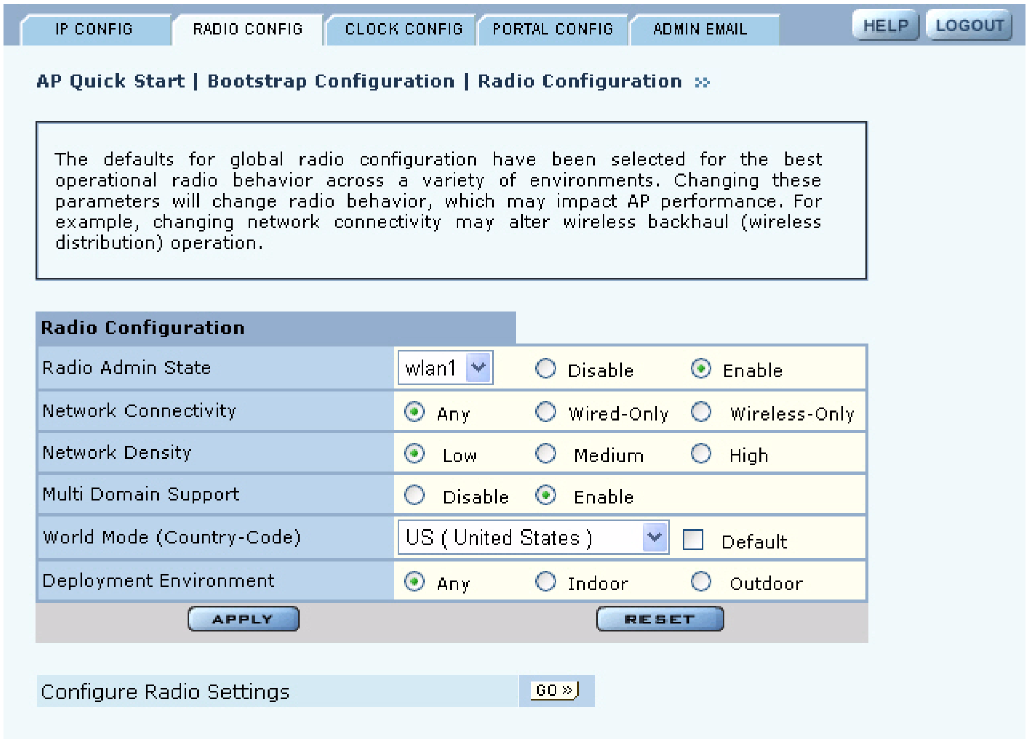
Field	Description
DNS IP Address	Enter the IP address of the server or servers supplying DNS service. This is required if the IP address is not obtained automatically. The default is the DNS server for the existing network. Multiple DNS server addresses may be specified, space-separated. The AP will use the addresses in the order specified. Manually configured DNS addresses always take precedence over the DNS addresses returned by a DHCP server. If the DNS IP Address field is empty, then all manually configured DNS server addresses will be removed. If you delete DNS servers, only those added manually are deleted. DHCP-assigned DNS servers continue to be available.
Management IP Address/Maskbits	Enter the IP address and subnet prefix for this AP. This is required if the IP address is not obtained automatically. The default is `192.168.1.254/24.`
Gateway IP Address	Enter the IP address of the gateway to the wired network. This is required if the IP address is not obtained automatically. The default is the existing network gateway.
Host Name	Enter an alphanumeric name for the AP. The factory default for this field is AP followed by the MAC address of the AP's Ethernet interface (eth0).
AP Location	Enter the physical location of the AP as a text string.
Administrator Contact	Enter contact information for the person responsible for managing this AP (phone or email address).

Click **Apply** to save changes in each section on the screen or **Reset** to return to previously saved values.

Radio Config Tab

Use the Radio Config tab (Figure 27) to configure bootstrap parameters for the two AP radios.

Figure 27: AP Quick Start - Bootstrap Configuration - Radio Config



AP Quick Start | Bootstrap Configuration | Radio Configuration »

The defaults for global radio configuration have been selected for the best operational radio behavior across a variety of environments. Changing these parameters will change radio behavior, which may impact AP performance. For example, changing network connectivity may alter wireless backhaul (wireless distribution) operation.

Radio Configuration			
Radio Admin State	wlan1	○ Disable	● Enable
Network Connectivity	● Any	○ Wired-Only	○ Wireless-Only
Network Density	● Low	○ Medium	○ High
Multi Domain Support	○ Disable	● Enable	
World Mode (Country-Code)	US (United States)	□ Default	
Deployment Environment	● Any	○ Indoor	○ Outdoor

Configure Radio Settings

This tab contains the following settings:

Field	Description
Radio Admin State	Select each AP radio (wlan0 or wlan1) to enable or disable.
Network Connectivity	Indicate whether the radio will be used in a normal AP connected to the wired network (Wired-Only), for wireless backhaul (Wireless-Only), or may be used for either (Any). If Any is specified, the system will automatically choose one.
Network Density	Indicate the relative concentration of APs in the network. For closely spaced APs that can support high data rates, select the high density option. For maximum coverage at lower data rates, selection the low density option. The default setting is Low.
Multi Domain Support	Enable or disable 802.11d operation. If Enable is selected, the radio advertises country, channel and associated maximum transmit power information in beacons and probes responses to stations or clients in the BSS. The default setting is enabled.
World Mode - Country Code	Select **Default** to set the channel and power for the radio to the factory default country setting (U.S.). Alternatively, enter a country code.
World Mode - Deployment Environment	Specify the type of environment in which the AP is installed (indoor, outdoor, or both). The Environment setting determines the maximum transmit power and allowed channels of operation.

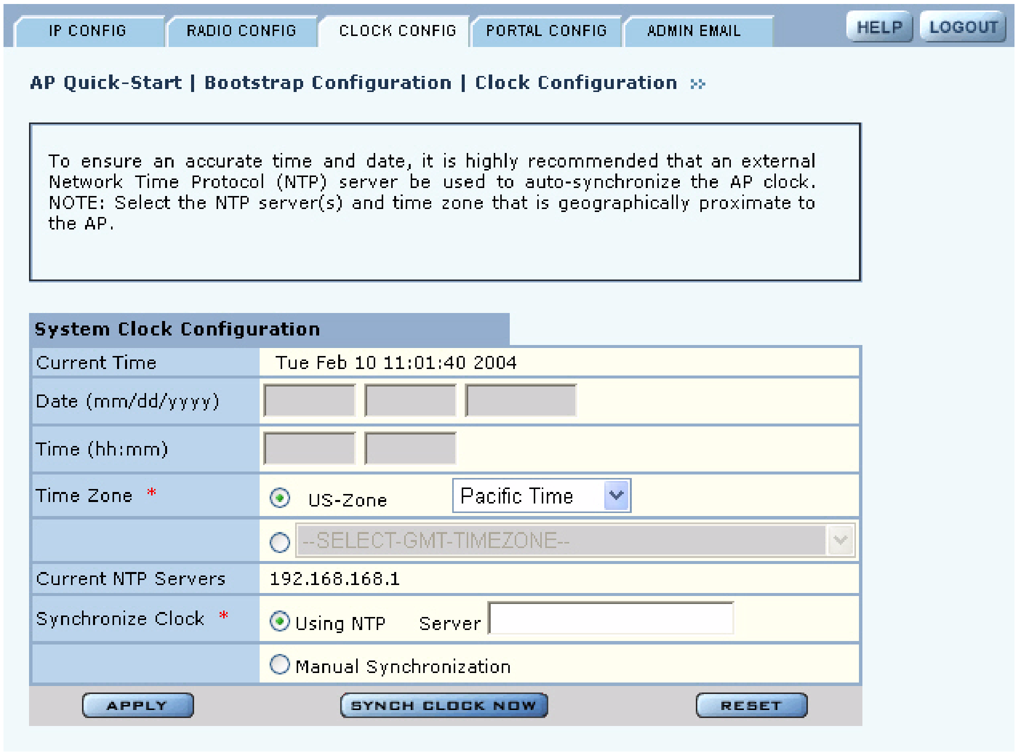
Field	Description
Configure Channel	Select Auto-Select Channel or Assign Fixed Channel options: • Auto-Select: Select At Start-up to automatically determine the channel when the AP is booted, or Periodic to auto-select the channel at the specified number of minutes. The default is Periodic and 30 minutes. • Assign Fixed Channel: Select a static channel. In both of these cases, the channel set used for auto-scanning can also be restricted.

For further information regarding these settings, see Chapter 4, "Configuring Radio Settings."

Clock Config Tab

Use the Clock Config tab (Figure 28) to set time parameters for the bootstrap configuration.

Figure 28: AP Quick Start - Bootstrap Configuration - Clock Config



AP Quick-Start | Bootstrap Configuration | Clock Configuration

To ensure an accurate time and date, it is highly recommended that an external Network Time Protocol (NTP) server be used to auto-synchronize the AP clock. NOTE: Select the NTP server(s) and time zone that is geographically proximate to the AP.

System Clock Configuration

Current Time	Tue Feb 10 11:01:40 2004
Date (mm/dd/yyyy)	
Time (hh:mm)	
Time Zone *	● US-Zone Pacific Time
	○ --SELECT-GMT-TIMEZONE--
Current NTP Servers	192.168.168.1
Synchronize Clock *	● Using NTP Server
	○ Manual Synchronization

This tab contains the following settings:

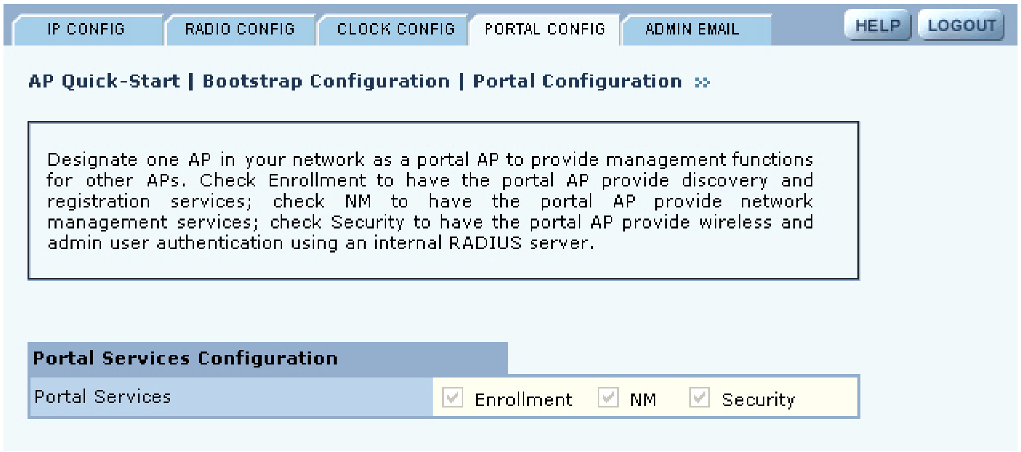
Field	Description
Date	Current date in MM/DD/YYYY format
Time	Current time in HH:MM:SS format (hours 0-23)
Time Zone	US-zone or GMT option. For US zone, click the radio button and select a time zone. For GMT, click the radio button and select an offset in HH:MM format.

Field	Description
Synchronize Clock	Indicate whether time will be synchronized manually through the date and time fields, or by way of an NTP server. If you select the server option, enter the IP address of the server in the space provided. If an NTP is currently assigned, the address of the server is displayed, as shown in Figure 28. Multiple NTP servers may be specified (space separated). If more than one server is specified, they are contacted in the order given. If the Synchronize Clock is empty, then all manually configured NTP servers will be deleted. If the AP is configured to receive an IP address via DHCP, then the DHCP server could also return the set of NTP servers. In such a scenario the manually configured NTP servers take precedence over the DHCP returned NTP servers. If you delete NTP servers, only those added manually are deleted. DHCP-assigned NTP servers continue to be available.

Portal Config Tab

Use the Portal Config tab (Figure 29) to enable portal services on this AP. See “Portal Architecture” on page 4 for a description of the portal services.

Figure 29: AP Quick Start - Bootstrap Configuration - Portal Config



AP Quick-Start | Bootstrap Configuration | Portal Configuration »

Designate one AP in your network as a portal AP to provide management functions for other APs. Check Enrollment to have the portal AP provide discovery and registration services; check NM to have the portal AP provide network management services; check Security to have the portal AP provide wireless and admin user authentication using an internal RADIUS server.

Portal Services Configuration

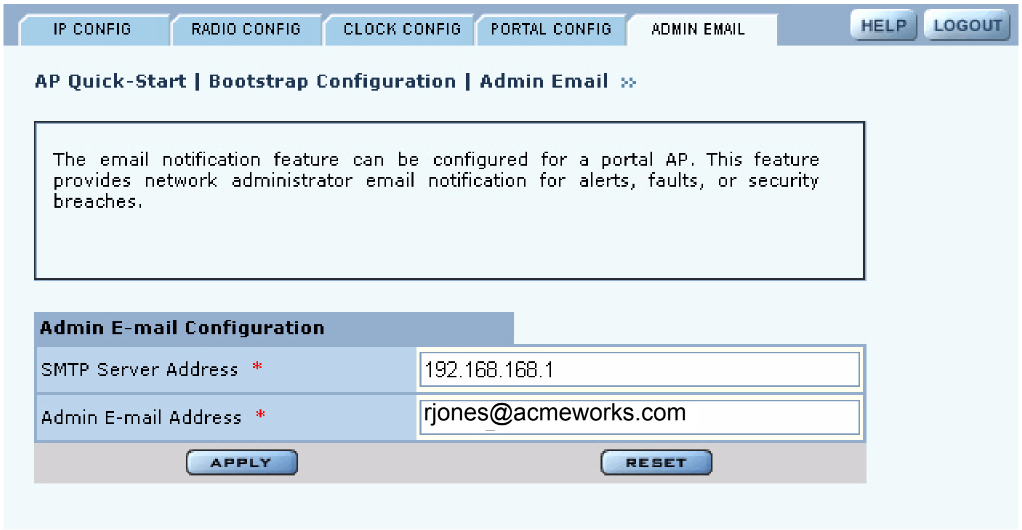
Portal Services	☑ Enrollment ☑ NM ☑ Security

Admin Email Tab

If the AP is configured as a portal AP, use the Admin Email tab (Figure 30) to specify how to alert the network administrator regarding critical faults or security breaches. Configure the following fields:

Field	Description
SMTP Server Address	Enter the IP address of the SMTP server used to reach the network administrator.
Admin E-mail Address	Enter the email address of the network administrator.

Figure 30: AP Quick Start - Bootstrap Configuration - Admin Email



AP Quick-Start | Bootstrap Configuration | Admin Email

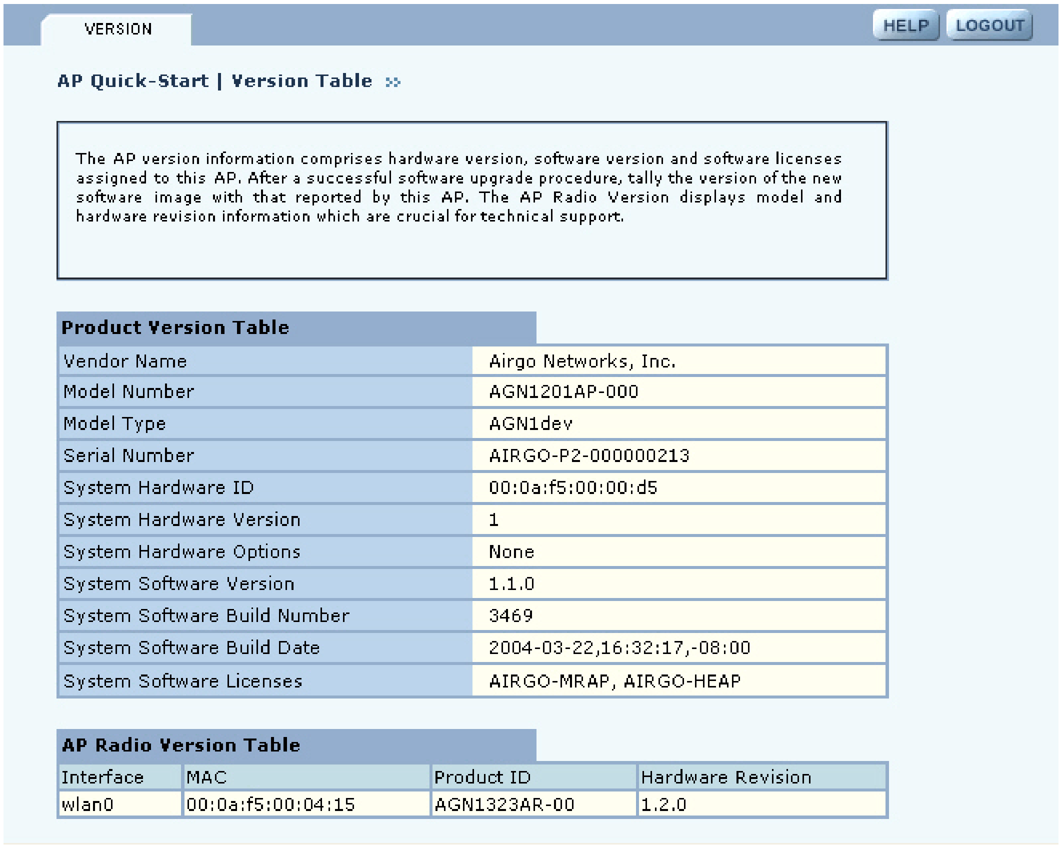
The email notification feature can be configured for a portal AP. This feature provides network administrator email notification for alerts, faults, or security breaches.

Admin E-mail Configuration	
SMTP Server Address *	192.168.168.1
Admin E-mail Address *	rjones@acmeworks.com

Version Table

The Version Table panel (Figure 25) lists model number, serial number, and hardware and software version information.

Figure 31: AP Quick Start - Version Table



AP Quick-Start | Version Table

The AP version information comprises hardware version, software version and software licenses assigned to this AP. After a successful software upgrade procedure, tally the version of the new software image with that reported by this AP. The AP Radio Version displays model and hardware revision information which are crucial for technical support.

Product Version Table	
Vendor Name	Airgo Networks, Inc.
Model Number	AGN1201AP-000
Model Type	AGN1dev
Serial Number	AIRGO-P2-000000213
System Hardware ID	00:0a:f5:00:00:d5
System Hardware Version	1
System Hardware Options	None
System Software Version	1.1.0
System Software Build Number	3469
System Software Build Date	2004-03-22,16:32:17,-08:00
System Software Licenses	AIRGO-MRAP, AIRGO-HEAP

AP Radio Version Table

Interface	MAC	Product ID	Hardware Revision
wlan0	00:0a:f5:00:04:15	AGN1323AR-00	1.2.0

Other Panels

The other panels accessible from the menu tree contain detailed information and fields to set the AP configuration. Most of the panels have multiple tabs, and some have special entry panels.

NM Portal Access

If the AP is booted in Portal mode, the left side of the browser interface includes a Manage Wireless Network button just below the menu tree. Click the button to open a new browser window for NM Portal services. For information on using portal services, see Chapter 9, "Managing the Network."

Configuration Wizards

The 108 Mbps Wireless AP web interface includes wizards that enable fast configuration of user security and guest access.

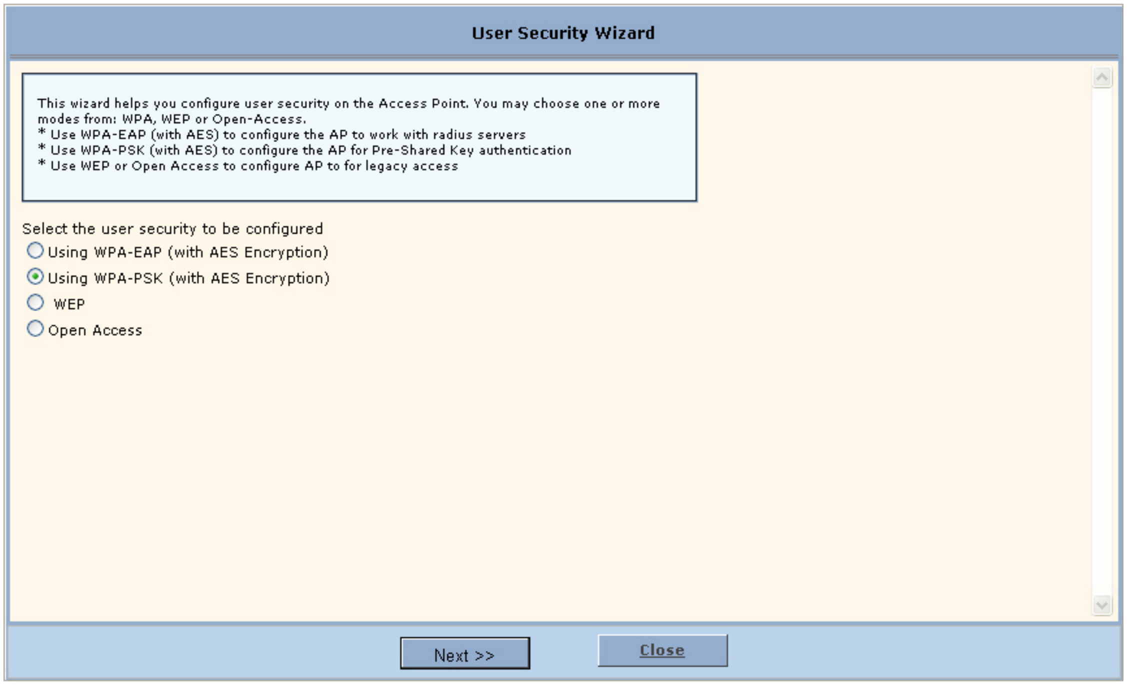
User Security Wizard

The User Security wizard provides a one-stop interface for configuring user security parameters. You can use the wizard to configure security or make changes to individual security screens in the AP web browser interface. For detailed information on security options, see Chapter 7, "Managing Security."

To open the User Security wizard:

Click **User Security Wizard** under AP Quick Start on the side menu. The User Access wizard opens (Figure 32).

Figure 32: User Security Wizard



User Security Wizard

This wizard helps you configure user security on the Access Point. You may choose one or more modes from: WPA, WEP or Open-Access.
* Use WPA-EAP (with AES) to configure the AP to work with radius servers
* Use WPA-PSK (with AES) to configure the AP for Pre-Shared Key authentication
* Use WEP or Open Access to configure AP to for legacy access

Select the user security to be configured

○ Using WPA-EAP (with AES Encryption)
● Using WPA-PSK (with AES Encryption)
○ WEP
○ Open Access

The wizard presents several options for configuring user security. For additional information about these options, see Chapter 7, "Managing Security."

Option	Description
WPA-EAP (with AES encryption)	Configures the AP to work with RADIUS authentication servers. • The wizard prompts for selection of the internal RADIUS server included in the AP or an external RADIUS server.
WPA-PSK	Configures the AP to work with pre-shared key authentication. • The wizard prompt for the pre-shared security key.
WEP	Configures the AP to use WEP encryption to support legacy equipment. • The wizard prompts for selection of 64-bit or 128-bit key length option, up to four distinct WEP keys, and determination of which will be the default.
Open Access	Configures the AP with no authentication or encryption. • The wizard prompts for confirmation that this is desired.

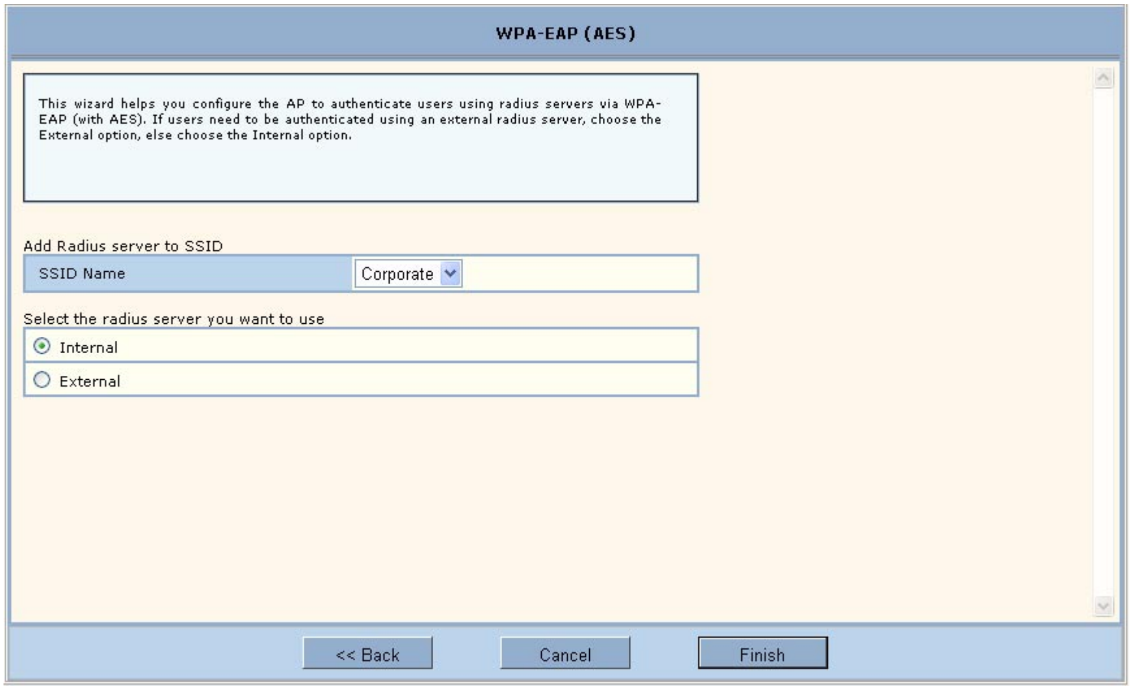
The security option you select determines the next step of the User Security wizard.

To configure WPA-EAP:

1 In the User Security Wizard, select **Using WPA-EAP.**

2 Click **Next** to open the next User Security wizard panel (Figure 33).

Figure 33: User Security Wizard - WPA-EAP



WPA-EAP (AES)

This wizard helps you configure the AP to authenticate users using radius servers via WPA-EAP (with AES). If users need to be authenticated using an external radius server, choose the External option, else choose the Internal option.

Add Radius server to SSID

SSID Name	Corporate

Select the radius server you want to use

● Internal

○ External

3 Confirm the SSID (wireless network name).

4 Select whether to use the internal RADIUS server included in the AP or an external RADIUS server.

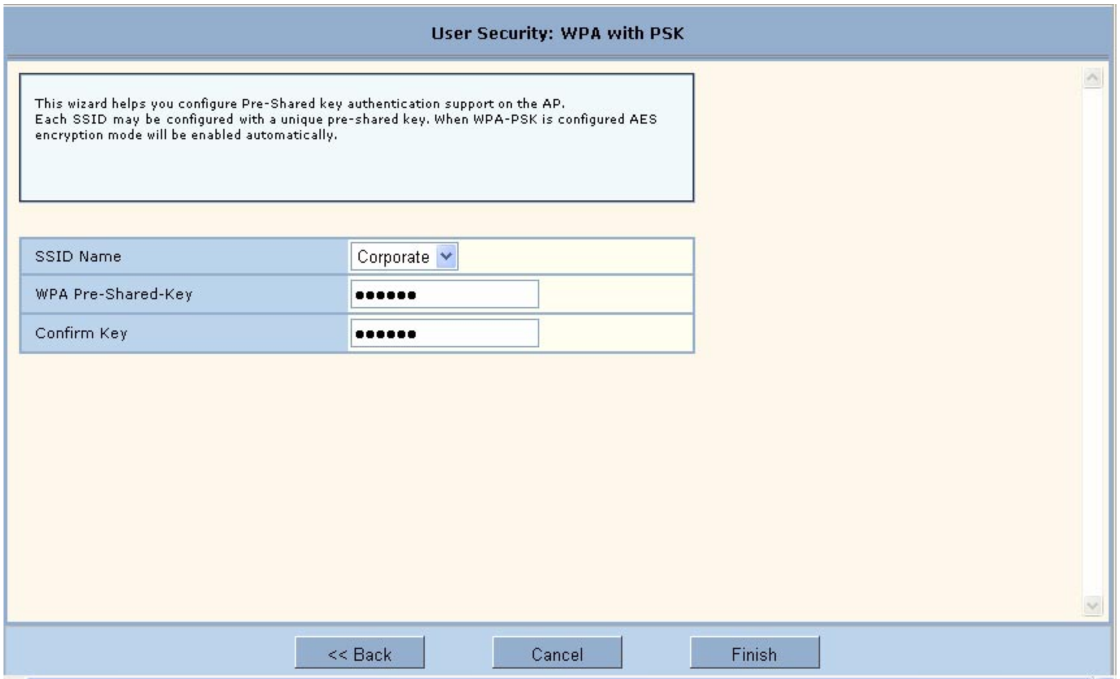
5 Click **Finish**.

To configure WPA-PSK:

1 In the User Security Wizard, select **Using WPA-PSK.**

2 Click **Next** to open the next User Security wizard panel (Figure 34).

Figure 34: User Security Wizard - WPA-PSK



User Security: WPA with PSK

This wizard helps you configure Pre-Shared key authentication support on the AP.
Each SSID may be configured with a unique pre-shared key. When WPA-PSK is configured AES encryption mode will be enabled automatically.

SSID Name	Corporate
WPA Pre-Shared-Key	••••••
Confirm Key	••••••

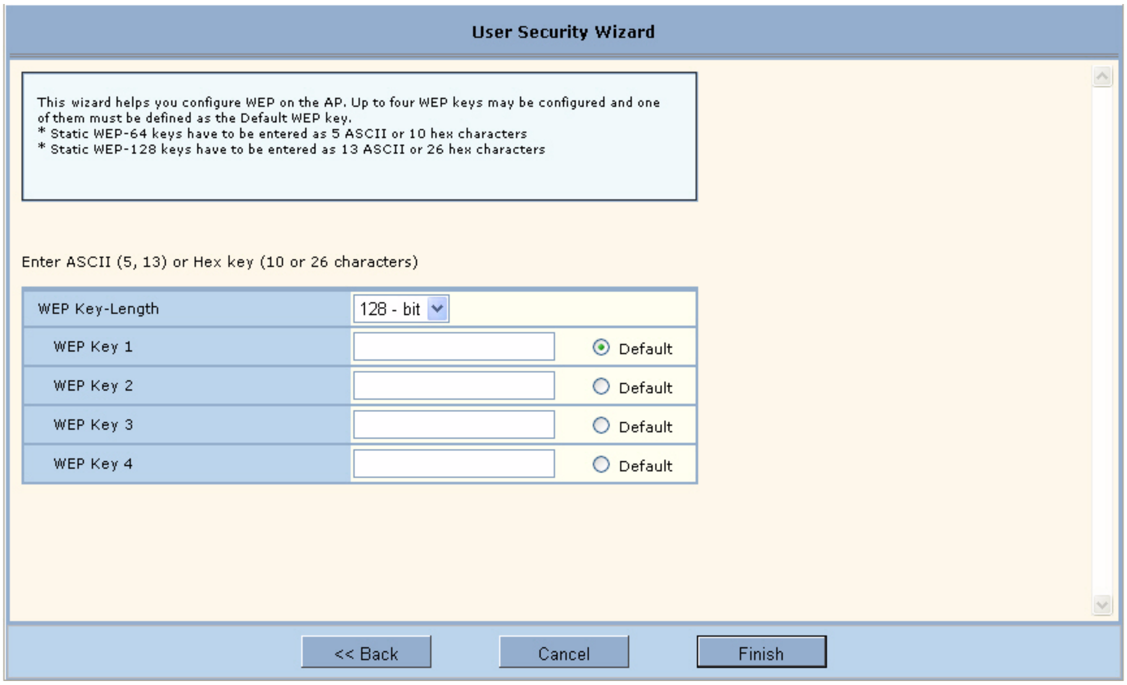
3 Enter the pre-shared key to use for network authentication and confirm your entry.

4 Click **Finish**.

To configure WEP:

1 Select **Using WEP,** and click **Next** to open the next User Security wizard panel (Figure 35).

Figure 35: User Security Wizard - WEP



User Security Wizard

This wizard helps you configure WEP on the AP. Up to four WEP keys may be configured and one of them must be defined as the Default WEP key.
* Static WEP-64 keys have to be entered as 5 ASCII or 10 hex characters
* Static WEP-128 keys have to be entered as 13 ASCII or 26 hex characters

Enter ASCII (5, 13) or Hex key (10 or 26 characters)

WEP Key-Length	128 - bit	
WEP Key 1		● Default
WEP Key 2		○ Default
WEP Key 3		○ Default
WEP Key 4		○ Default

2 Select the WEP key length.

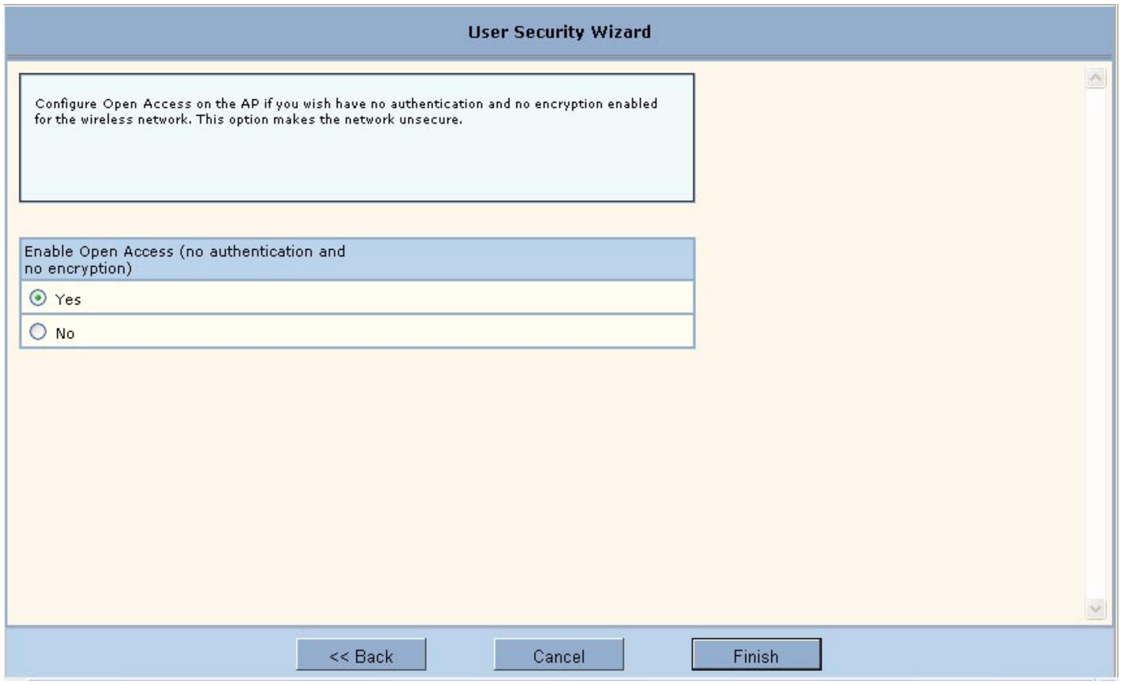
3 Enter up to four WEP keys, and indicate which will be the default.

4 Click **Finish**.

To configure open access:

1 Select **Open Access,** and click **Next** to open the next User Security wizard panel (Figure 36).

Figure 36: User Security Wizard - Open Access



User Security Wizard

Configure Open Access on the AP if you wish have no authentication and no encryption enabled for the wireless network. This option makes the network unsecure.

Enable Open Access (no authentication and no encryption)

● Yes

○ No

2 Confirm that you want to configure the AP without user security.

3 Click **Finish**.

Guest Access Wizard

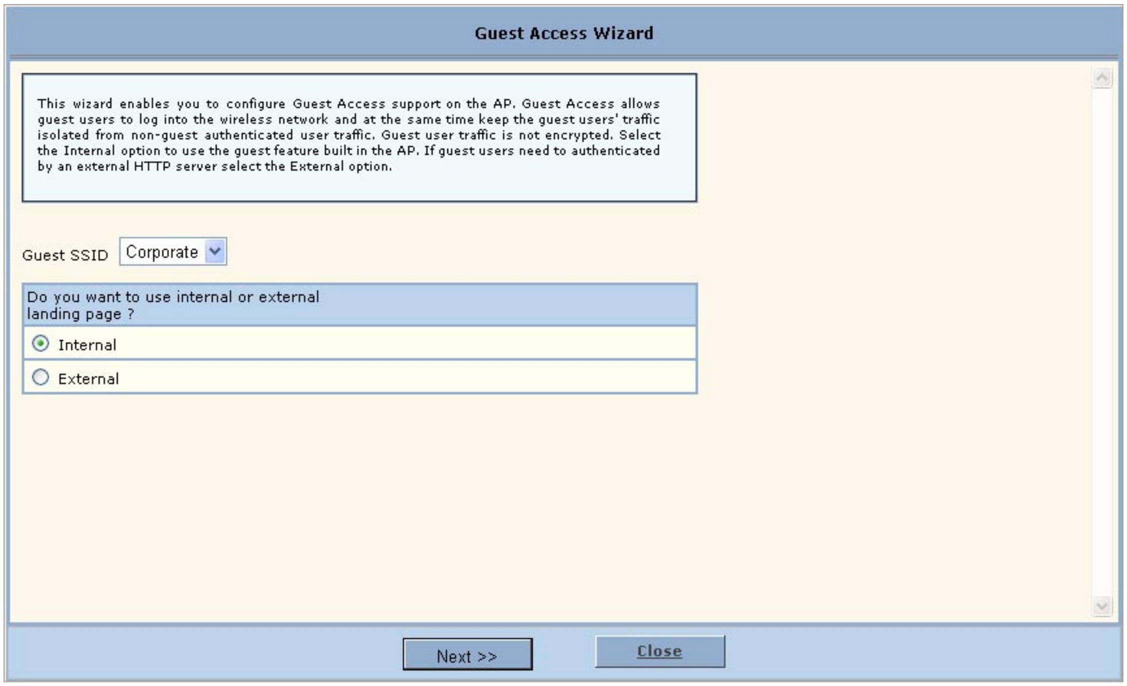
The Guest Access wizard enables you to configure the network to give guest users limited access while protecting the network from unauthorized use. For a complete description of guest access rules and options, see Chapter 8, "Configuring Guest Access."

To open the Guest Access wizard:

- Click **Guest Access Wizard** under AP Quick Start on the side menu.

The wizard (Figure 37) provides options to configure an internal landing page or an external landing page for users who open a web browser while on site.

Figure 37: Guest Access Wizard



Guest Access Wizard

This wizard enables you to configure Guest Access support on the AP. Guest Access allows guest users to log into the wireless network and at the same time keep the guest users' traffic isolated from non-guest authenticated user traffic. Guest user traffic is not encrypted. Select the Internal option to use the guest feature built in the AP. If guest users need to authenticated by an external HTTP server select the External option.

Guest SSID: Corporate

Do you want to use internal or external landing page ?

● Internal

○ External

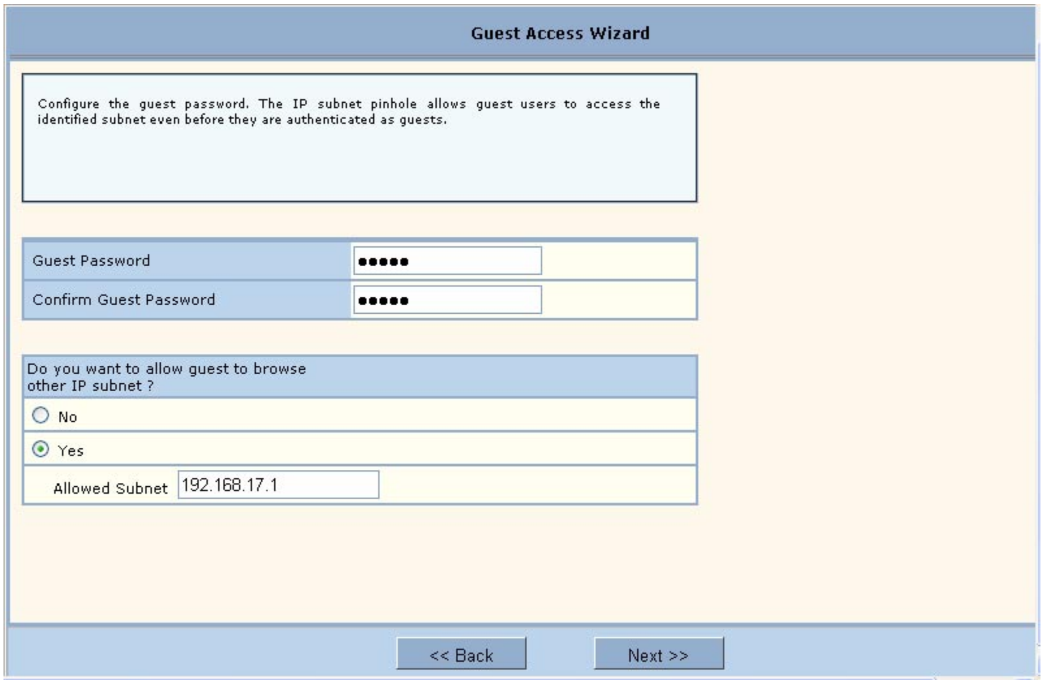
To use an internal landing page:

1 In the Guest Access wizard, select **Internal**.

2 Click **Next** to open the next wizard panel.

3 Enter and confirm a guest password (Figure 38). The password must be from 1 to 63 characters in length and may be manually distributed to guests who visit your corporate facility.

Figure 38: Guest Access Wizard - Internal Landing Page



Guest Access Wizard

Configure the guest password. The IP subnet pinhole allows guest users to access the identified subnet even before they are authenticated as guests.

Guest Password	●●●●●
Confirm Guest Password	●●●●●

Do you want to allow guest to browse other IP subnet ?

○ No

◉ Yes

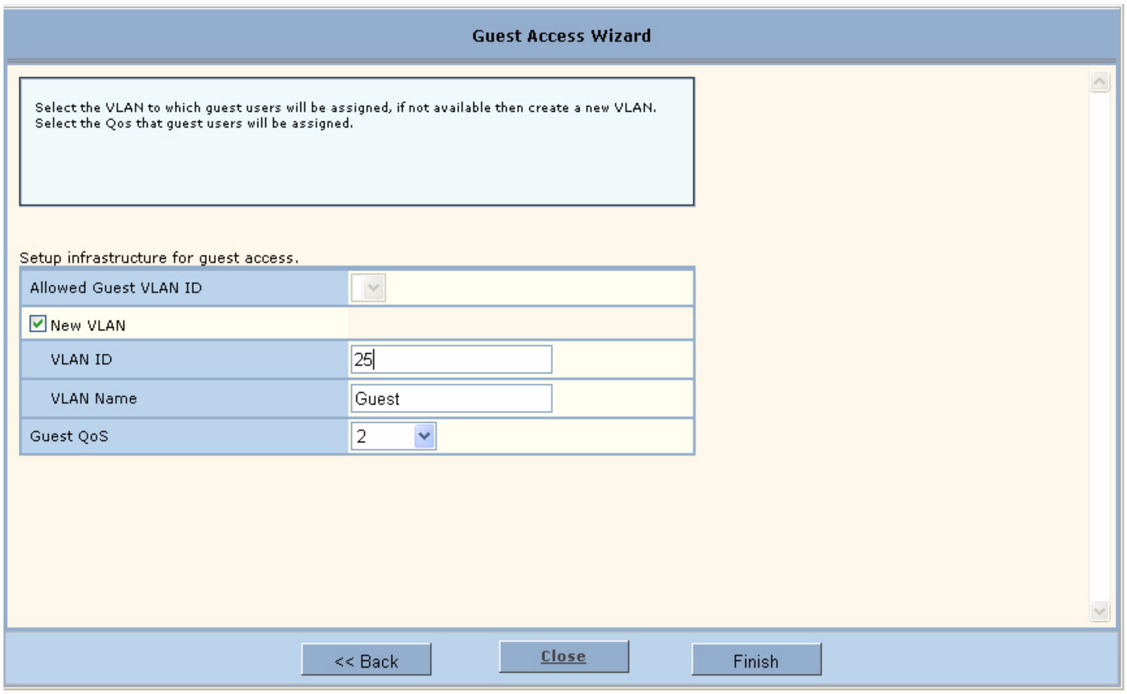
Allowed Subnet 192.168.17.1

4 Indicate whether the guest users will be able to access a subnet before they are authenticated as guest users. If yes, enter the IP address of the subnet.

5 Click **Next**.

6 Select an existing VLAN in which to place authenticated guest users, or create a new VLAN by entering a numeric VLAN ID and VLAN name (Figure 39). The list of existing VLANS includes only those that support open access.

Figure 39: Guest Access Wizard - VLAN Entry



Guest Access Wizard

Select the VLAN to which guest users will be assigned, if not available then create a new VLAN.
Select the Qos that guest users will be assigned.

Setup infrastructure for guest access.

Allowed Guest VLAN ID	
☑ New VLAN	
VLAN ID	25
VLAN Name	Guest
Guest QoS	2

7 Click **Finish**.

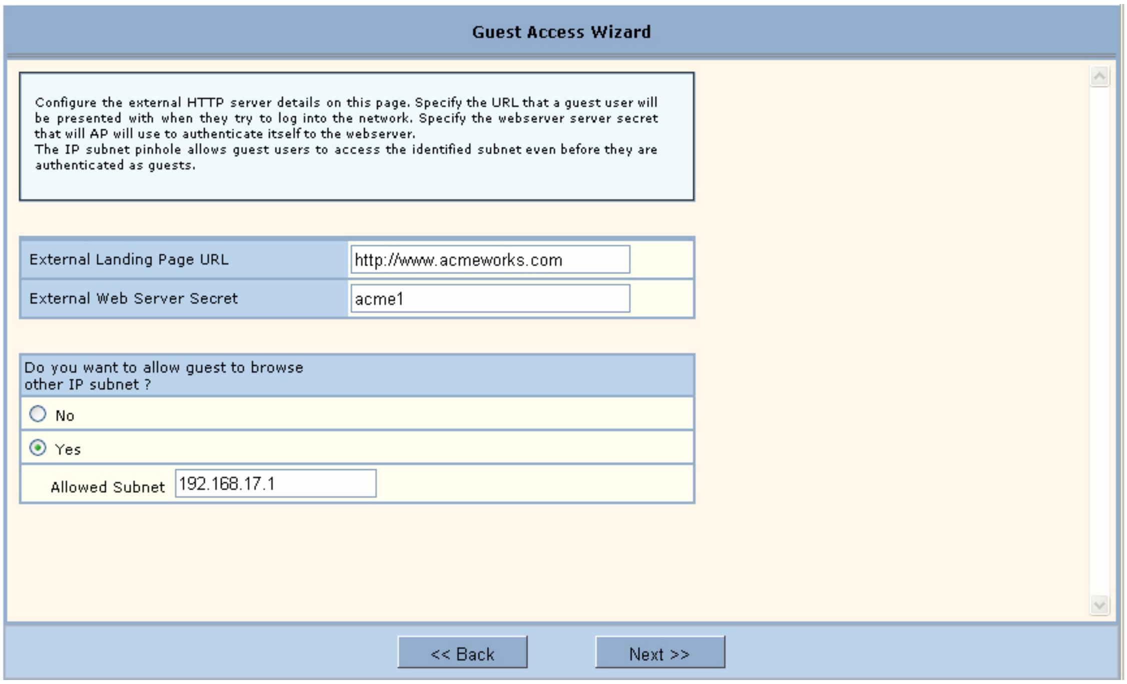
Guest access is now configured. When guests access the external landing page, they follow an externally-determined process to log in to the network. If a subnet has been specified, then guests can access the subnet even if they are not able to log in. For further information about guest access, or to modify guest access parameters, see Chapter 7, "Managing Security."

To use an external landing page:

1 In the Guest Access wizard, select **External**.

2 Click **Next** to open the next wizard panel.

Figure 40: Guest Access Wizard - External Landing Page



Guest Access Wizard

Configure the external HTTP server details on this page. Specify the URL that a guest user will be presented with when they try to log into the network. Specify the webserver server secret that will AP will use to authenticate itself to the webserver.
The IP subnet pinhole allows guest users to access the identified subnet even before they are authenticated as guests.

External Landing Page URL	http://www.acmeworks.com
External Web Server Secret	acme1

Do you want to allow guest to browse other IP subnet ?

○ No

● Yes

Allowed Subnet 192.168.17.1

3 Enter the full URL for the external landing page (Figure 39). The URL for the landing page must use an IP address rather than a domain name. Regardless of the authentication process selected for the external page, it is necessary to forward authentication results to the AP upon completion of successful or unsuccessful guest authentication. The 108 Mbps Wireless Access Point is shipped with an sample external landing page.

4 Enter the shared secret string that the AP will use to authenticate itself to the web server. The code must be from 1 to 63 characters in length.

5 Indicate whether the guest users will be able to access a subnet before they are authenticated as guest users. If yes, enter the IP address of the subnet.

6 Click **Next**.

7 Select an existing VLAN in which to place authenticated guest users, or create a new VLAN by entering a numeric VLAN ID and VLAN name (Figure 39 on page 52). The list of existing VLANS includes only those that support open access.

8 If desired, select a quality of service (QoS) level. Numeric QoS values range from 0 (lowest priority) to 7 (highest priority).

9 Click **Finish**.

Guest access is now configured. When guests access the external landing page, they follow an externally-determined process to log in to the network. If a subnet has been specified, then guests can access the subnet even if they are not able to log in. For further information about guest access, or to modify guest access parameters, see Chapter 7, “Managing Security.”

4 Configuring Radio Settings

This chapter describes the configuration settings for the 108 Mbps Wireless Access Point radios and explains how to set the configuration using the 108 Mbps Wireless AP web interface. It covers all the features accessible from the Wireless Services menu except backhaul configuration, which is discussed in Chapter 6. The chapter includes the following topics:

- **Introduction**
- **Configuring Radio Parameters**
- **Setting the Advanced Radio Configuration**
- **Viewing Radio Statistics**
- **Viewing Radio Neighbor Details**
- **Configuring SSID Parameters**
- **Multiple SSIDs**
- **Configuring Inter Access Point Protocol (IAPP)**
- **Performing Radio Diagnostics**

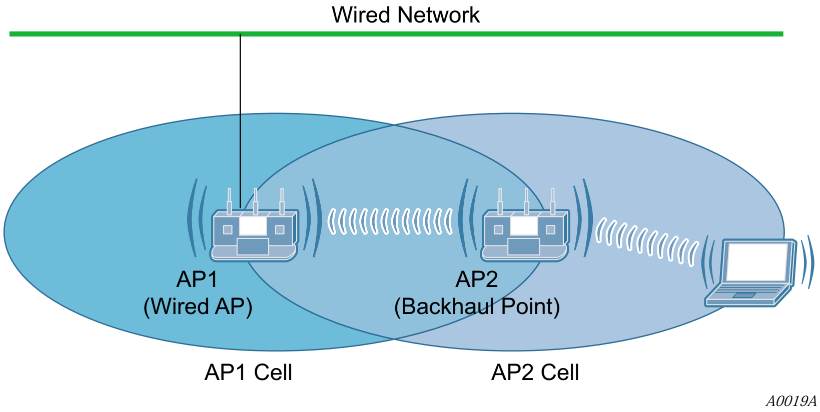
Introduction

The 108 Mbps Wireless Access Point can be configured with one or two radios, each of which forms a distinct wireless cell or basic service set (BSS), as shown in Figure 41. Each radio can operate in either of the following modes:

- In normal mode, the AP is connected to the wired network, and the radio directly services downstream client stations or access points, or both. (AP mode).
- In wireless backhaul mode, the radio establishes a wireless link to a radio in AP mode on another 108 Mbps Wireless AP in order to relay data through the wireless medium. The AP is not attached to a wired connection, instead it is connected through the wireless medium to another AP.[1] In this mode, the radio is called a Backhaul Point (BP mode). Wireless backhaul is also known as a wireless distribution system (WDS).

[1] Except in certain special configurations.

Figure 41: AP Radios and Coverage



Use the Wireless Services items on the menu tree to access wireless parameters. The following rules apply to the wireless settings:

- Some of the settings apply globally (for both radios); others apply on a per-radio basis.
- For configuration and reference purposes, the individual radios are labeled `wlan0` and `wlan1`. The wired Ethernet interface is labeled `eth0`.
- Some of the commands apply only to one mode (AP or BP).
- If the radio is in BP mode, parameters are stored and later applied if and when the radio takes on the AP mode.

Each of the items in the Wireless Services menu leads to a specific area of radio configuration:

Menu Item	**Description**
Radio Configuration	General radio parameters
Advanced Configuration	802.11 mode for each radio
Radio State & Statistics	Detailed status and statistics for each radio
Radio Neighbors	Identity of neighboring APs within beacon range
SSID Configuration	Identification of the SSID parameters and assignment of service profiles
Backhaul Configuration	Configuration of wireless backhaul links (See Chapter 6, "Configuring a Wireless Backhaul.")
Station Management	List of stations associated to the 108 Mbps Wireless AP
IAPP Configuration	Configuration of Inter-Access Point Protocol for roaming and load balancing
Radio Diagnostics	Interface to perform link and walk tests

To open one of the Wireless Services panels, choose the topic from the menu tree.

Configuring Radio Parameters

Choose **Radio Configuration** from the Wireless Services menu to open the AP Radio Configuration panel. The panel contains the following tabs:

- Global Configuration—Set parameters that apply to both of the AP radios.
- Persona Configuration—Set the radio mode or persona for normal (AP) operation or wireless backhaul (BP).

- Channel Configuration—Configure channel usage for each radio.
- Performance—Configure enhanced data rates and performance attributes.
- Admission—Specify categories of client stations that are permitted to associate to the selected radio.

To configure settings on these tabs, select each in sequence, or step through using the Go links at the bottom of the panel (shown in Figure 42).

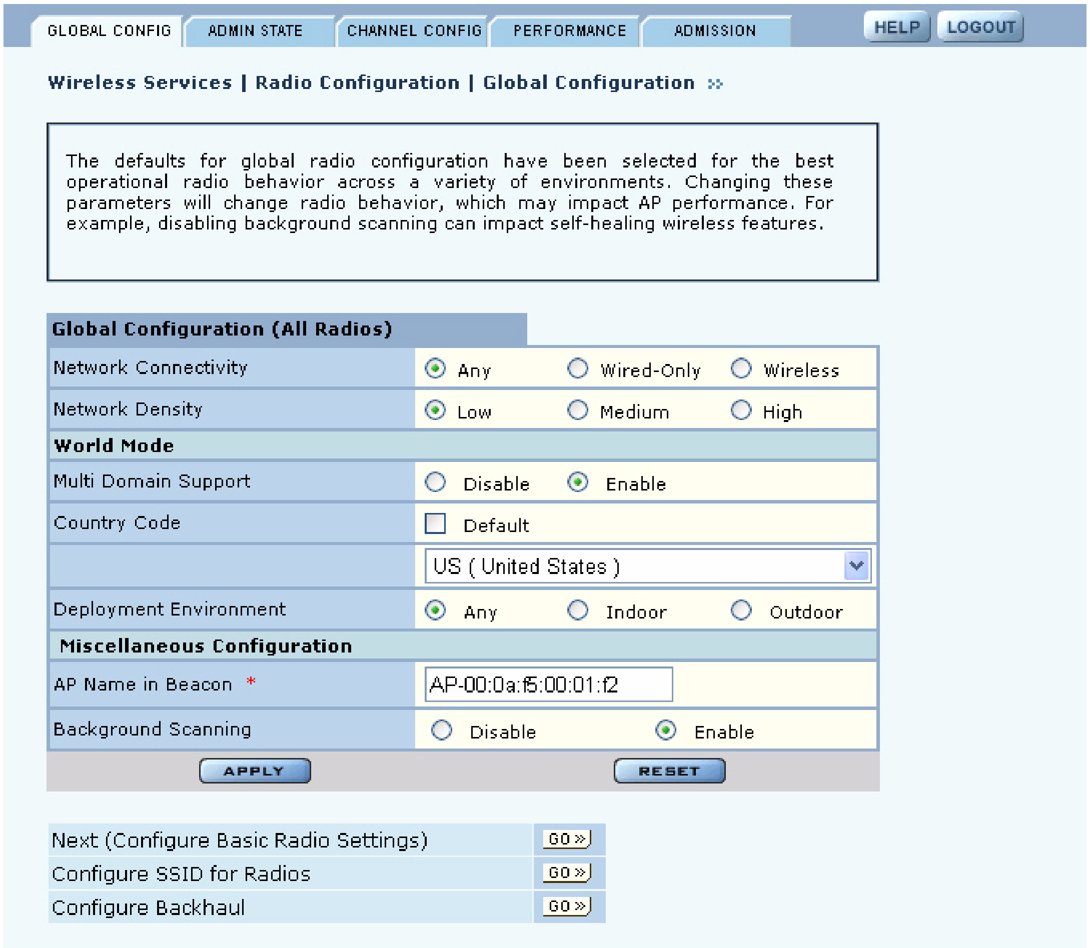
Many of the radio parameters are interdependent, and the 108 Mbps Wireless AP performs consistency checks during configuration to prevent user actions from adversely affecting radio performance. This is especially true of dual radio APs, due to the proximity of the two radios. If you attempt to make configuration changes that are not accepted by the AP, an error message may or may not appear. Consult the appropriate section in this chapter to determine which parameters are in conflict.

Global Configuration

Use the Global Configuration tab (Figure 42) to define settings that apply to both of the 108 Mbps Wireless AP radios.

NOTE: All the settings on this tab are optional. If the AP radio is enabled when the global configuration is changed, then it is necessary to reset the AP for the changes to take effect. If the radio is disabled, the changes take effect once the radio is enabled.

Figure 42: Radio Configuration - Global Config



Wireless Services | Radio Configuration | Global Configuration »

The defaults for global radio configuration have been selected for the best operational radio behavior across a variety of environments. Changing these parameters will change radio behavior, which may impact AP performance. For example, disabling background scanning can impact self-healing wireless features.

Global Configuration (All Radios)	
Network Connectivity	● Any ○ Wired-Only ○ Wireless
Network Density	● Low ○ Medium ○ High
World Mode	
Multi Domain Support	○ Disable ● Enable
Country Code	□ Default
	US (United States)
Deployment Environment	● Any ○ Indoor ○ Outdoor
Miscellaneous Configuration	
AP Name in Beacon *	AP-00:0a:f5:00:01:f2
Background Scanning	○ Disable ● Enable

Next (Configure Basic Radio Settings)	GO »
Configure SSID for Radios	GO »
Configure Backhaul	GO »

Set the following global parameters on this tab:

Field	Description
Network Connectivity	Specify the mode of connectivity to the wired network. • The default value of Any means that the AP auto-determines whether or not to initiate a backhaul based on the presence or absence of an active Ethernet link. The Any setting is influenced by the number of radios in the 108 Mbps Wireless AP and whether or not the AP has active Ethernet connectivity. If Any is selected, then the 108 Mbps Wireless AP is allowed to change between wireless and wired mode based on a change in Ethernet status. • The Wired-Only setting means that the 108 Mbps Wireless AP operates only as wired node. The node is disabled if the Ethernet link is not active. All radios take on the AP persona unless explicitly configured as a BP radio. • The Wireless value means that the AP operates only as a wireless backhaul node with wireless backhaul connectivity to the wired network. One radio is automatically assigned the BP persona and one the AP persona. Applies to dual radio APs only. The default setting of Any is recommended.

Field (continued)	Description
Network Density	Set the wireless network density (low, medium, or high). Moving APs closer to each other increases wireless capacity by providing higher data rates to clients. To support this configuration, select the high density option. For maximum coverage at lower data rates, use the low density setting. Each setting determines the defer threshold parameters for the 108 Mbps Wireless AP. The default is low; the default setting of "low" is appropriate for maximum coverage.
World Mode - Multi-Domain Support	Enables or disables 802.11d operation. If Enable is selected, the radio advertises country, channel and associated maximum transmit power information in beacons and probes responses to stations or clients in the BSS. The default setting is enabled.
World Mode - Country Code	Specify the country of operation of the AP. Select **Default** to set the channel and power for the radio to the factory default country setting (U.S.). Alternatively, enter a country code from the pull-down menu.
World Mode - Deployment Environment	Specify the type of environment in which the AP is installed (indoor, outdoor, or both). Choosing the environment and country influences the channels of operation that the AP or BP operate in or use for scanning and the maximum radio transmit power. If the country or environment is changed, the following occur: • The channel selection setting is reset to auto-select channel at startup. To configure a radio on a specific channel, apply the country configuration and then specify the channel using the Channel Configuration tab (see "Channel Configuration" on page 65). • The channel set configuration is set to system determined band configuration. • All radios in the AP are reset. For reference, Table 8 provides a list of world modes, including countries, environments, bands, and valid channels.
AP Name in Beacon	Confirm the AP node name advertised in beacons and probe responses. This is the AP name that clients see when they scan for access points. The default is the unique ID derived from the Ethernet MAC address of the AP. It is recommended to accept the default setting. (required, AP radio only)
Background Scanning	Enable or disable background scanning. Background scanning is performed to collect interference and radio neighbor information from the surrounding RF environment. If auto-select-channel is enabled with the Periodic option, background scanning should also be enabled. See "Channel Configuration" on page 65.

Click **Apply** to save changes or **Reset** to return to previously saved values.

Table 8:World Modes

Country	Environment	Band	Valid Channel Numbers
USA	Any	2.4	1,2,3,4,5,6,7,8,9,10,11
USA	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11
USA	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11
USA	Any	5	52,56,60,64,149,153,157,161
USA	Indoor	5	36,40,44,48,52,56,60,64,149,153,157,161
USA	Outdoor	5	52,56,60,64,149,153,157,161

Table 8:World Modes (continued)

Country	Environment	Band	Valid Channel Numbers
Mexico	Any	2.4	1,2,3,4,5,6,7,8,9,10,11
Mexico	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11
Mexico	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11
Mexico	Any	5	149,153,157,161
Mexico	Indoor	5	36,40,44,48,52,56,60,64,149,153,157,161
Mexico	Outdoor	5	149,153,157,161
Argentina	Any	2.4	1,2,3,4,5,6,7,8,9,10,11
Argentina	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11
Argentina	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11
Argentina	Any	5	52,56,60,64,149,153,157,161
Argentina	Indoor	5	52,56,60,64,149,153,157,161
Argentina	Outdoor	5	52,56,60,64,149,153,157,161
Brazil	Any	2.4	1,2,3,4,5,6,7,8,9,10,11
Brazil	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11
Brazil	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11
Brazil	Any	5	149,153,157,161
Brazil	Indoor	5	149,153,157,161
Brazil	Outdoor	5	149,153,157,161
Countries listed under the leading Europe include major European countries not explicitly listed by name in this table.			
Europe	Any	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Europe	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Europe	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Europe	Any	5	100,104,108,112,116,120,124,128,132,126,140
Europe	Indoor	5	36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,126,140
Europe	Outdoor	5	100,104,108,112,116,120,124,128,132,126,140
France	Any	2.4	9
France	Indoor	2.4	9
France	Outdoor	2.4	9
France	Any	5	Not allowed
France	Indoor	5	36,40,44,48,52,56,60,64
France	Outdoor	5	9,10,11,12,13
Austria	Any	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Austria	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Austria	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Austria	Any	5	Not allowed
Austria	Indoor	5	36,40,44,48,52,56,60,64
Austria	Outdoor	5	Not Allowed

Table 8:World Modes (continued)

Country	Environment	Band	Valid Channel Numbers
Belgium	Any	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Belgium	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Belgium	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Belgium	Any	5	Not allowed
Belgium	Indoor	5	36,40,44,48,52,56,60,64
Belgium	Outdoor	5	Not Allowed
Spain	Any	2.4	10,11
Spain	Indoor	2.4	10,11
Spain	Indoor	2.4	10,11
Spain	Any	5	100,104,108,112,116,120,124,128,132,126,140
Spain	Indoor	5	36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132, 126,140
Spain	Outdoor	5	100,104,108,112,116,120,124,128,132,126,140
Switzerland	Any	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Switzerland	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Switzerland	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13
Switzerland	Any	5	Not allowed
Switzerland	Indoor	5	36,40,44,48
Switzerland	Outdoor	5	Not Allowed
Japan	Any	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13,14
Japan	Indoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13,14
Japan	Outdoor	2.4	1,2,3,4,5,6,7,8,9,10,11,12,13,14
Japan	Any	5	34,38,42,46
Japan	Indoor	5	34,38,42,46
Japan	Outdoor	5	34,38,42,46
Singapore	Any	2.4	9,10,11,12,13
Singapore	Indoor	2.4	9,10,11,12,13
Singapore	Outdoor	2.4	9,10,11,12,13
Singapore	Any	5	52,56,60,64,149,153,157,161
Singapore	Indoor	5	36,40,44,48,52,56,60,64,149,153,157,161
Singapore	Outdoor	5	52,56,60,64,149,153,157,161
Israel	Any	2.4	4,5,6,7,8,9
Israel	Indoor	2.4	4,5,6,7,8,9
Israel	Outdoor	2.4	4,5,6,7,8,9
Israel	Any	5	52,56,60,64,149,153,157,161

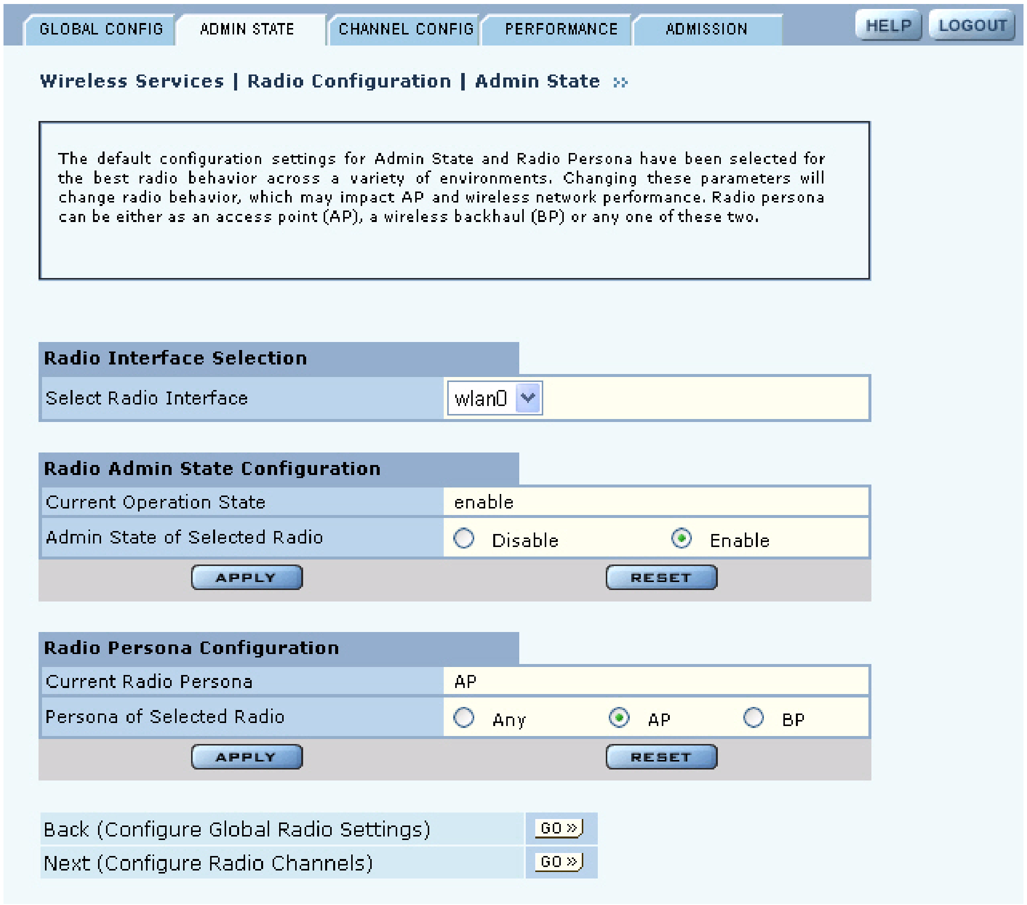
Table 8:World Modes (continued)

Country	Environment	Band	Valid Channel Numbers
Israel	Indoor	5	36,40,44,48,52,56,60,64,149,153,157,161
Israel	Outdoor	5	52,56,60,64,149,153,157,161

Admin State Configuration

Use the Admin State tab (Figure 43) to assign the mode or persona of each radio interface.

Figure 43: Radio Configuration - Admin State



The default configuration settings for Admin State and Radio Persona have been selected for the best radio behavior across a variety of environments. Changing these parameters will change radio behavior, which may impact AP and wireless network performance. Radio persona can be either as an access point (AP), a wireless backhaul (BP) or any one of these two.

Radio Interface Selection

Select Radio Interface	wlan0

Radio Admin State Configuration

Current Operation State	enable
Admin State of Selected Radio	○ Disable ● Enable

Radio Persona Configuration

Current Radio Persona	AP
Persona of Selected Radio	○ Any ● AP ○ BP

Back (Configure Global Radio Settings)	GO »
Next (Configure Radio Channels)	GO »

Set the following parameters on this tab:

Feature	Description
Select Radio Interface	Select the AP radio (wlan0 or wlan1)
Admin State of Selected Radio	Enable or disable the selected radio. When the AP radio is in the disabled state, all valid configuration settings are saved. When the AP radio is enabled, the latest configuration is applied. It is not possible to disable the BP radio by administrative intervention. (AP radio only)
Persona of Selected Radio	Select whether the AP radio is to operate as a normal AP (AP) or in backhaul point mode (BP). Select **Any** to determine the radio mode automatically based on network connectivity, configuration, number of radios, and presence of Ethernet connectivity. It is recommended to accept the default setting of Any.

NOTE: Each access point can have at most one BP radio.

Click **Apply** to save changes or **Reset** to return to previously saved values. Click **Reset Radio to Default** to return the settings on all the radios to their factory defaults.

Interdependencies

If Network Connectivity on the Radio Global tab ("Global Configuration" on page 57) is set to Wireless, then at least one radio must have the BP or Any persona. If the Network Connectivity setting is Wired or Any, then the personas of AP, BP, and Any are all permitted.

Table 9 shows how the Network Connectivity setting on the Global Configuration tab relates to the Radio Persona Configuration on the Admin state tab.

Table 9: Radio Settings for Network Connectivity and Persona

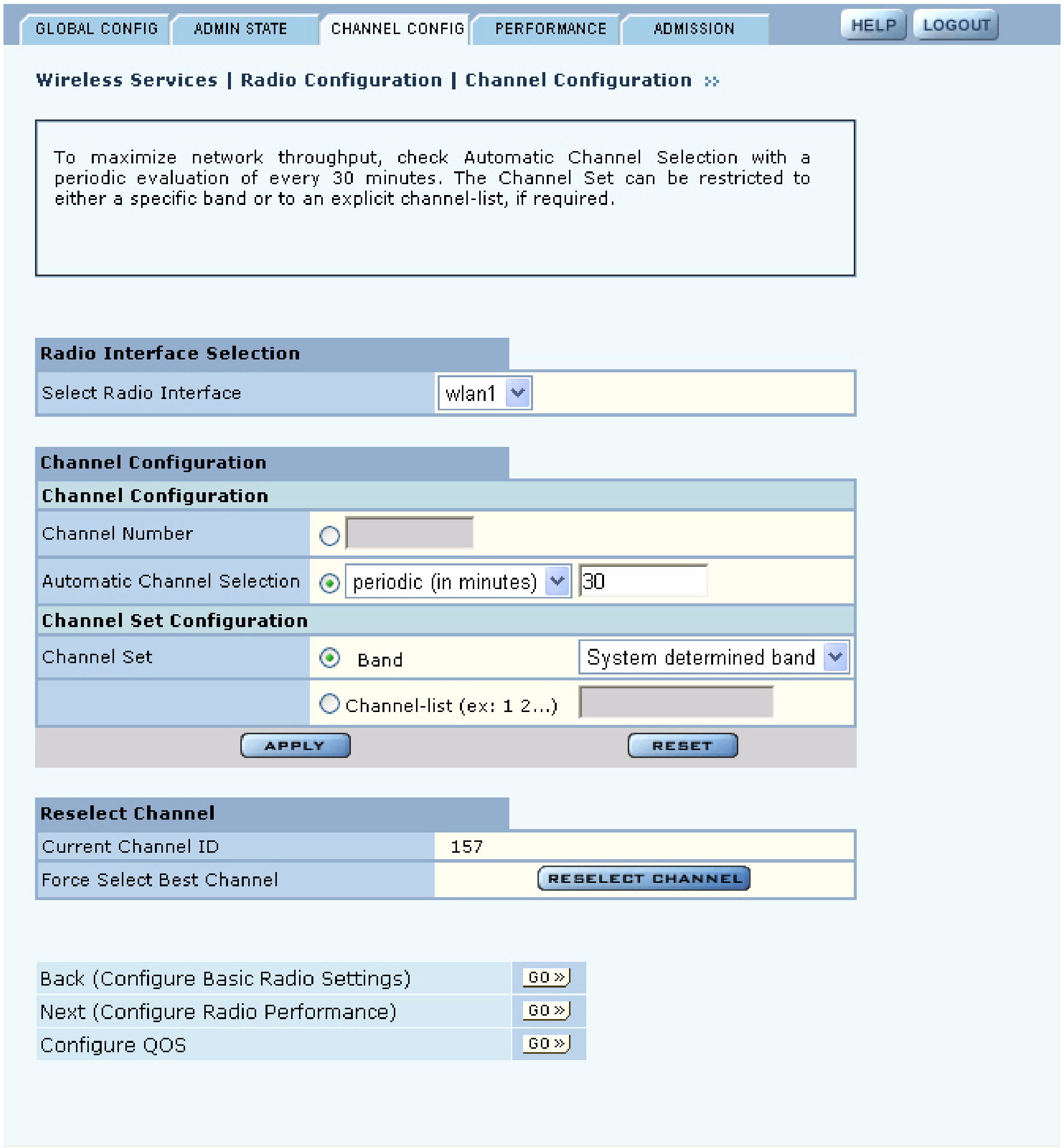
Number of Radios	Wired Connection[a]	Network Connectivity Setting	Persona Setting	Resulting radio persona or mode
One	Yes	Any	Any or AP	AP
One	Yes	Any	BP	BP
Two	Yes	Any	All combinations of Any and AP	Both radios AP
Two	Yes	Any	All combinations that specify a BP radio	1 radio AP, 1 radio BP
Two	No	Any	One radio set as BP	1 radio AP, 1 radio BP
Two	No	Any	Both radios AP	Not permitted
One	Yes	Wired	Any	AP
Two	Yes	Wired	All combinations of Any and AP	Both radios AP
Two	No	Wireless	All combinations except both radios AP	1 radio AP, 1 radio BP
Two	No	Wireless	Both radios AP	Not permitted

[a] Wired Connection means that the AP has Ethernet connectivity and that the connection is active.

Channel Configuration

Use the Channel Configuration tab (Figure 44) to define rules for selecting radio channels. If two radios are installed in the same AP, each radio operates in a different band (2.4 GHz for one radio and 5 GHz for the other).

Figure 44: Radio Configuration - Channel Config



Wireless Services | Radio Configuration | Channel Configuration »

To maximize network throughput, check Automatic Channel Selection with a periodic evaluation of every 30 minutes. The Channel Set can be restricted to either a specific band or to an explicit channel-list, if required.

Radio Interface Selection

Select Radio Interface	wlan1

Channel Configuration

Channel Configuration

Channel Number	○	
Automatic Channel Selection	● periodic (in minutes)	30

Channel Set Configuration

Channel Set	● Band	System determined band
	○ Channel-list (ex: 1 2...)	

Reselect Channel

Current Channel ID	157
Force Select Best Channel	RESELECT CHANNEL

Back (Configure Basic Radio Settings)

Next (Configure Radio Performance)

Configure QOS

Set the following values in the Radio Interface Selection and Channel Configuration areas of the tab:

Feature	Description
Select Radio Interface	Select the AP radio (wlan0 or wlan1).
Channel Number	Select a valid channel for radio operation, or accept the Automatic Channel Selection option.

Feature (continued)	Description
Automatic channel selection	Specify whether the channel is chosen when the AP is started, or whether it is selected periodically. The time range for periodic channel selection is 30 minutes to 24 hours (1440 minutes). It is recommended to accept the default setting of automatic channel selection of periodic at 30 minutes.
Channel Set	Determine which channels the AP scans in order to determine the best channel for operation. If Auto-Selection is enabled, this determines the channel set for auto-selection. The following choices are available for channel set: Band—Select a specific band, or the system-determined band option (recommended). • The System Determined Band setting means that the system chooses the channel list or band for each radio based on the number of AP radios, the persona of the radio, and the channel set of any second radio in the AP. If the radio is in AP mode, then the node selects the best channel across both bands. If the radio is in BP mode, then the BP radio scans on both bands. • If the 108 Mbps Wireless AP is configured with two AP radios and Auto-Selection is chosen for both, then the preferred band configuration for both radios is System Determined. If both radios are in AP mode, then one operates in the 2.4 GHz band and the other in the 5 GHz band. • If the Channel Set is 2.4 or 5GHz, then the AP radio operates only in the specified band. If it is set to 2.4 GHz, the AP chooses only non-overlapping channels for operation (for example 1, 6, and 11). It is not acceptable to set both radios to operate in the 2.4 GHz or 5GHz band. • If both bands are selected, the AP radio chooses the best channel based on the mode and band of the other radio on the AP (if installed). • If a BP radio establishes a backhaul in the same band as the other AP radio, this triggers the AP radio to change bands, provided that the AP radio is configured for auto-selection and the system determined band. Channel List—Enter a specific list of channels to be scanned, separated by a single space (e.g.,1 2 6 11 13...). Overlapping channels can be specified in the 2.4 GHz band.

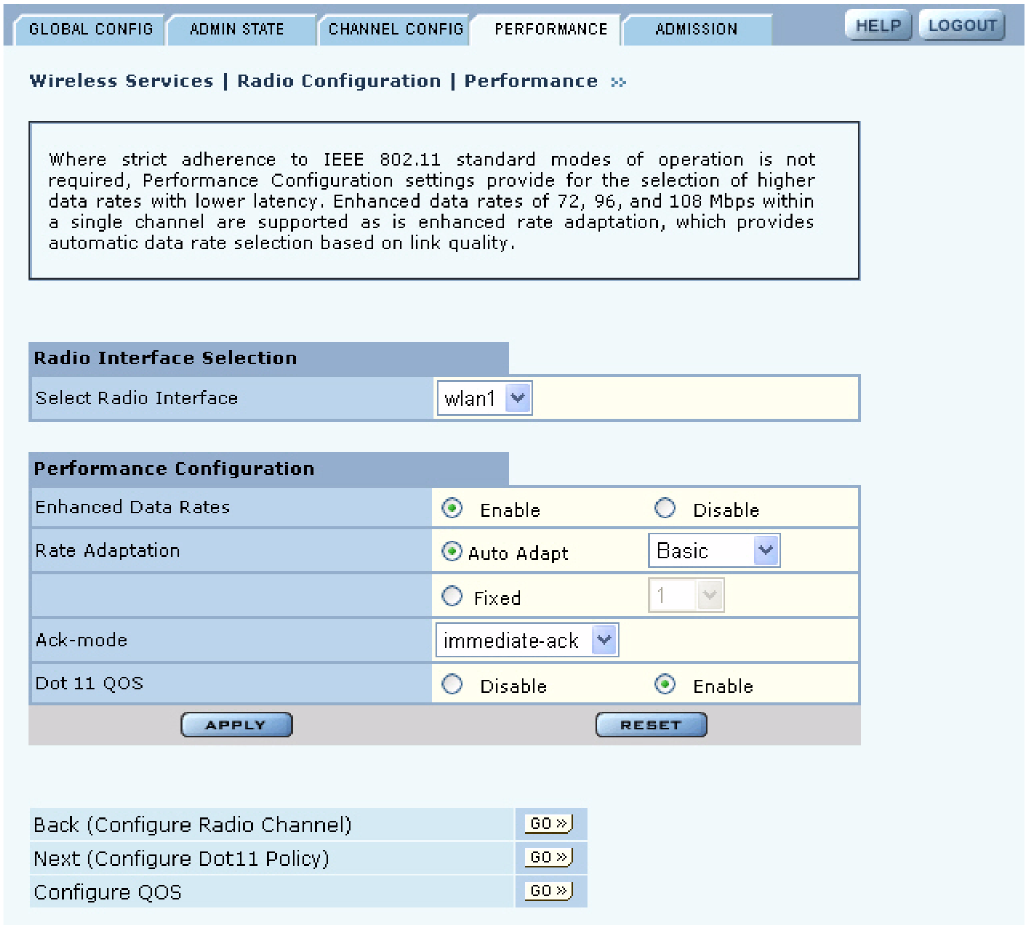
ℹ **NOTE:** World mode and environment settings influence the channel and channel set configurations. See “Global Configuration” on page 57 for information on world modes.

Click **Apply** to save changes or **Reset** to return to previously saved values. Click **Force Select Best Channel** to trigger the channel selection algorithm for the AP radio, including a switch-over to a better channel, if available. The Force Select Reselect Channel button applies only to the selected AP radio interface.

Performance

Use the Performance tab (Figure 45) to configure enhanced data rates of 72, 96, or 108 Mbps.

Figure 45: Radio Configuration - Performance



Wireless Services | Radio Configuration | Performance »

Where strict adherence to IEEE 802.11 standard modes of operation is not required, Performance Configuration settings provide for the selection of higher data rates with lower latency. Enhanced data rates of 72, 96, and 108 Mbps within a single channel are supported as is enhanced rate adaptation, which provides automatic data rate selection based on link quality.

Radio Interface Selection	
Select Radio Interface	wlan1

Performance Configuration		
Enhanced Data Rates	● Enable	○ Disable
Rate Adaptation	● Auto Adapt	Basic
	○ Fixed	1
Ack-mode	immediate-ack	
Dot 11 QOS	○ Disable	● Enable

Back (Configure Radio Channel)
Next (Configure Dot11 Policy)
Configure QOS

Set the following values on this tab:

Feature	**Description**
Select Radio Interface	Select the AP radio (wlan0 or wlan1)
Enhanced Data Rates	Enable or disable the PLANEX enhanced data rates of (72, 96, and 108 Mbps). This setting is rejected if the enhanced Dot11 extensions are disabled and an attempt is made to configure enhanced data rates. It is recommended to accept the default of Enabled.
Rate Adaptation	Enables or disables automatic data rate adaptation in the system. To use auto-adaptation, select the Auto Adapt button and select the Basic or Advanced option. Otherwise, select fixed along with a fixed rate. It is recommended to accept the default value of Auto Adapt and Basic.

Feature (continued)	Description
Ack Mode	Determines the acknowledgement policy for data packets. The following selections are available: • Immediate Ack – Acknowledgement is sent for every packet received. This is the default setting. • No Ack – No acknowledgement is sent when data packets are received. • To enable high performance, use this setting together with one of the enhanced data rates. • If this setting is used, then auto-adaptation cannot be enabled for the selected radio. Only the fixed rate setting applies. • This mode setting can be used for operations with PLANEX clients. • Auto-ack – The acknowledgement policy is selected automatically based on current link conditions.
Dot11 QoS	Enables or disables 802.11e QoS. If enabled, the MAC mode is set to EDCF or HCF. If disabled, then the MAC mode is DCF. It is recommended to accept the default of Enabled.

Click **Apply** to save changes or **Reset** to return to previously saved values.

Interdependencies

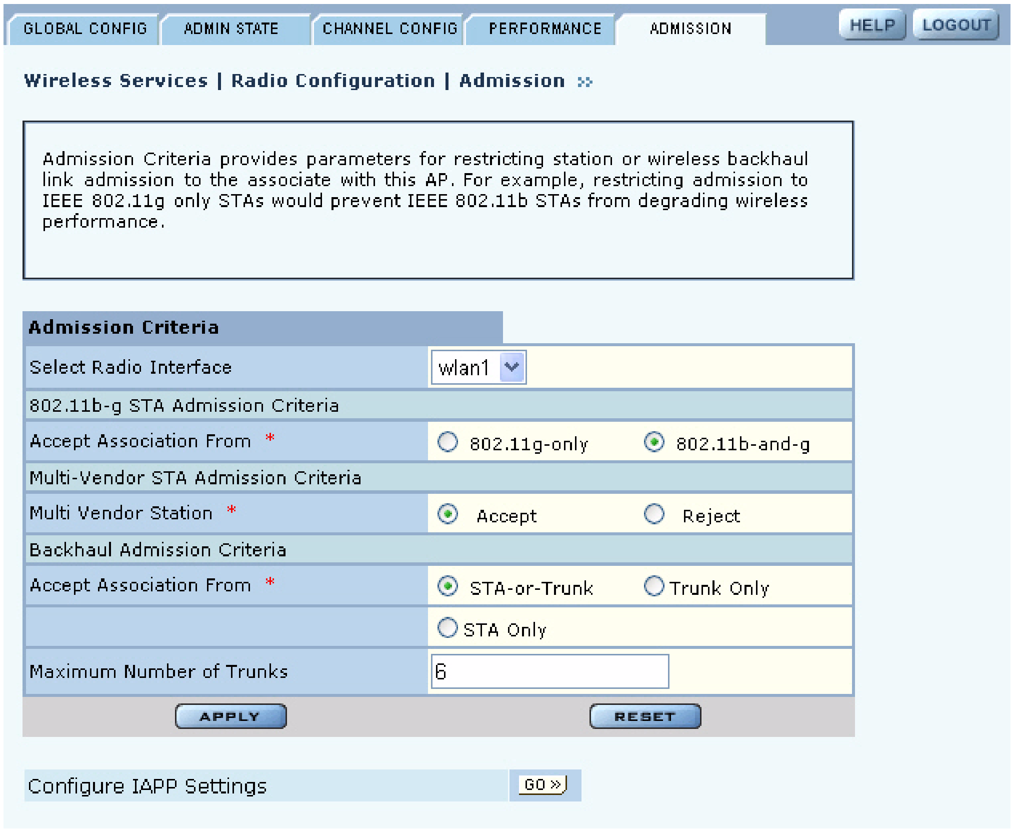
Some restrictions apply to combinations of settings on the Channel Configuration and Performance tabs.

- For fixed data rate configurations:
  - If the configured channel is in the 5 GHz band or the Channel Set Band/List is 5 GHz, System Determined, or Both, then at least one of the fixed rates must be other than an 11b rate (1,2,5.5,or 11).
  - If the configured channel is in the 2.4 GHz band or the Channel Set Band/List is 2.4 GHz only, then only 11b/g rates are accepted.
  - Assigning an enhanced rate (72, 96, and 108 Mbps), requires that the enhanced rates option be enabled.
- To enable the Dot11 QoS settings on the Performance tab, you must enable the standard Dot-11 extensions on the 802.11 Policy tab (see “802.11 Policy” on page 70).

Admission

Use the Admission tab (Figure 45) to specify categories of client stations that are permitted to associate to the selected radio.

Figure 46: Radio Configuration - Admission



Wireless Services | Radio Configuration | Admission »

Admission Criteria provides parameters for restricting station or wireless backhaul link admission to the associate with this AP. For example, restricting admission to IEEE 802.11g only STAs would prevent IEEE 802.11b STAs from degrading wireless performance.

Admission Criteria		
Select Radio Interface	wlan1	
802.11b-g STA Admission Criteria		
Accept Association From *	○ 802.11g-only	● 802.11b-and-g
Multi-Vendor STA Admission Criteria		
Multi Vendor Station *	● Accept	○ Reject
Backhaul Admission Criteria		
Accept Association From *	● STA-or-Trunk	○ Trunk Only
	○ STA Only	
Maximum Number of Trunks	6	

Configure IAPP Settings

Set the following values on this tab:

Feature	Description
Select Radio Interface	Select the AP radio (wlan0 or wlan1).
802.11b-g STA Admission Criteria - Accept Association from	Applies to the 2.4 Ghz band only. Specify the type of 802.11g or 802.11b and g client stations permitted to associate. Selecting 802.11g-only keeps 802.11b stations from degrading BSS performance. 802.11b and g is the default setting.
Multi-Vendor STA Admission Criteria - Multi-Vendor Station	Accept allows all stations to associate; Reject restricts association to compatible client stations, excluding non-compatible or non-PLANEX stations.
Backhaul Admission Criteria - Accept Association From	Indicates whether to accept association from client stations, trunks or both: STA or Trunk—Accept association from client stations or BP radios. STA Only—Accept associations only from client stations. Trunk Only—Accept associations only from BP radios.
Max Number of Trunks	Determines the maximum number of trunks which are allowed to form with the AP radio (range is 1-10). Default is 6.

Setting the Advanced Radio Configuration

Select **Advanced Configuration** from the Wireless Services menu to open the Advanced Configuration feature panel. The panel contains the following tabs:

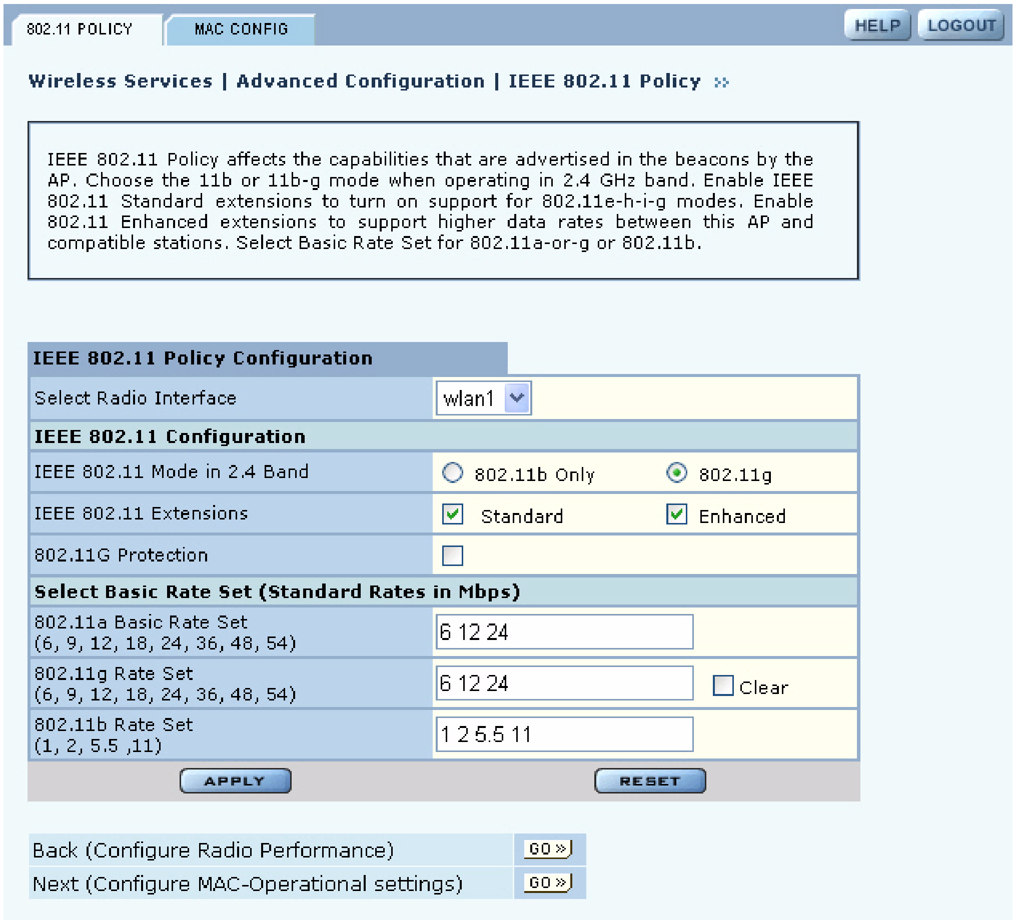
- 802.11 Policy—Set the 802.11 modes for the AP radios.
- MAC Config—Set details of the radio beacon and MAC configuration for each radio.

To configure settings on these tabs, select each in sequence, or step through the tabs using the Go links at the bottom of the panel (Figure 47).

802.11 Policy

Use the 802.11 tab(Figure 47) to set the 802.11 modes and data rates for each AP radio.

Figure 47: Advanced Configuration - 802.11 Policy



Wireless Services | Advanced Configuration | IEEE 802.11 Policy

IEEE 802.11 Policy affects the capabilities that are advertised in the beacons by the AP. Choose the 11b or 11b-g mode when operating in 2.4 GHz band. Enable IEEE 802.11 Standard extensions to turn on support for 802.11e-h-i-g modes. Enable 802.11 Enhanced extensions to support higher data rates between this AP and compatible stations. Select Basic Rate Set for 802.11a-or-g or 802.11b.

IEEE 802.11 Policy Configuration

Select Radio Interface	wlan1	
IEEE 802.11 Configuration		
IEEE 802.11 Mode in 2.4 Band	○ 802.11b Only	● 802.11g
IEEE 802.11 Extensions	☑ Standard	☑ Enhanced
802.11G Protection	□	
Select Basic Rate Set (Standard Rates in Mbps)		
802.11a Basic Rate Set (6, 9, 12, 18, 24, 36, 48, 54)	6 12 24	
802.11g Rate Set (6, 9, 12, 18, 24, 36, 48, 54)	6 12 24	□ Clear
802.11b Rate Set (1, 2, 5.5 ,11)	1 2 5.5 11	

Back (Configure Radio Performance)	GO »
Next (Configure MAC-Operational settings)	GO »

Set the following values on this panel:

Feature	Description
Select Radio Interface	Select the AP radio (wlan0 or wlan1).
IEEE 802.11 Mode in 2.4 Band	Select whether the radio is configured for 802.11b or 802.11g operation when it operates in the 2.4 GHz band.

Feature (continued)	Description
IEEE 802.11 Extensions	Indicate whether to support standard Dot11 extensions, enhanced extensions, or both. The checkboxes enable or disable standard 802.11 extensions such as 11h, 11e, 11g or 11i, or PLANEX enhanced features, which are compatible only with PLANEX client stations. If the Enhanced 802.11 extensions option is selected, then it is possible to enable the following through the CLI (they are not automatically enabled). • Enhanced rate set (specific flag needs to be set) • Proprietary burst ack • Advanced rate adaptation • Wireless backhaul AP name in beacon (if not enabled, the AP name in beacon is suppressed)
802.11G Protection	Select to enable 802.11g protection mode, short slot time, and short preamble if the radio is operating in 802.11g mode. If the checkbox is selected, all 3 aspects are enabled; if not, all 3 aspects are disabled. The default setting is disabled.
Select Basic Rate Set	Enter basic data rates for the different 802.11 modes. To set rates, select **Set** and enter the rates with a space as the delimiter. The basic 802.11 rates are advertised in beacons and inform the client stations of the minimum set of rates it must support to be part of the BSS. 802.11 control frames such as ACKS, CTS, and RTS are transmitted at basic rates.

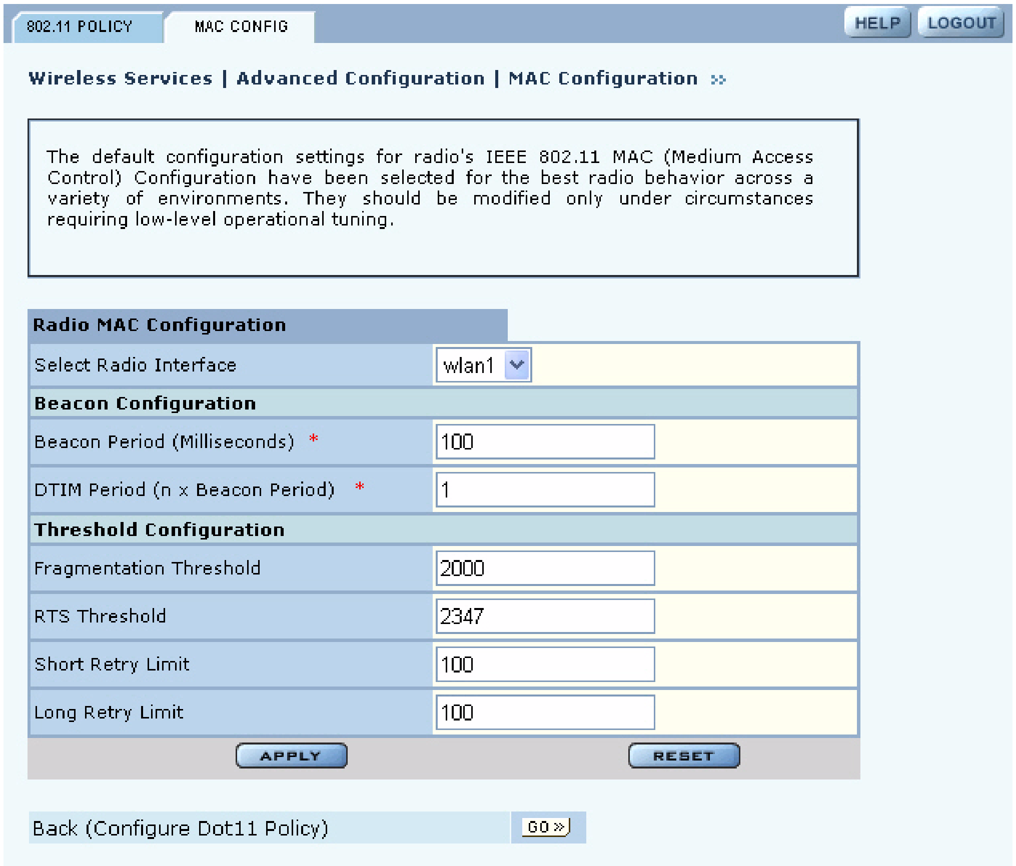
Click **Apply** to save changes or **Reset** to return to previously saved values.

MAC Configuration

Use the MAC Configuration tab (Figure 48) under special circumstances if it is necessary to tune low level operational parameters of the radio MAC (Medium Access Control) layer.

NOTE: Changes on the MAC Configuration tab should only be made by trained network personnel. The AP radio restarts automatically when these parameter changes are applied.

Figure 48: MAC Configuration Tab


802.11 POLICY
MAC CONFIG
HELP
LOGOUT
Wireless Services | Advanced Configuration | MAC Configuration »
APPLY
RESET
GO »

The default configuration settings for radio's IEEE 802.11 MAC (Medium Access Control) Configuration have been selected for the best radio behavior across a variety of environments. They should be modified only under circumstances requiring low-level operational tuning.

Radio MAC Configuration	
Select Radio Interface	wlan1
Beacon Configuration	
Beacon Period (Milliseconds) *	100
DTIM Period (n x Beacon Period) *	1
Threshold Configuration	
Fragmentation Threshold	2000
RTS Threshold	2347
Short Retry Limit	100
Long Retry Limit	100

Back (Configure Dot11 Policy)

Set the following parameters on the MAC Configuration tab:

Field	**Description**
Select Radio Interface	Select the AP radio (required, wlan0 or wlan1).
Beacon Period	Enter the desired interval between RF beacons, in milliseconds. It is recommended to accept the default of 100 ms. (required).
DTIM (Delivery Traffic Indication Message) Period	Enter the interval between the times that the radio forwards multicast and broadcast packets to client stations. It is recommended to accept the default of 1 beacon period. (required).
Fragmentation Threshold	Enter the maximum packet size that can be transmitting as a single unit. A low setting may be desirable in areas that have significant interference or poor signal conditions. The range is 256-2346. It is recommended to accept the default of 2000.
RTS Threshold	Enter a packet size greater than which the AP issues a request-to-send (RTS) message before sending the packet. Enter a low threshold if the ambient conditions might make it relatively difficult for clients to associate to the AP. The range is 0-2347. It is recommended to accept the default of 2347.
Short Retry Limit	Enter a number of transmission retries (greater than or equal to data frame MSDU size) after which a transmission is deemed a failure. The range is 1-255.
Long Retry Limit	Enter a number of transmission retries (greater than or equal to data frame MSDU size) after which a transmission is deemed a failure. The range is 1-255.

Click **Apply** to save changes or **Reset** to return to previously saved values. The changes take effect immediately if the radio is enabled.

Viewing Radio Statistics

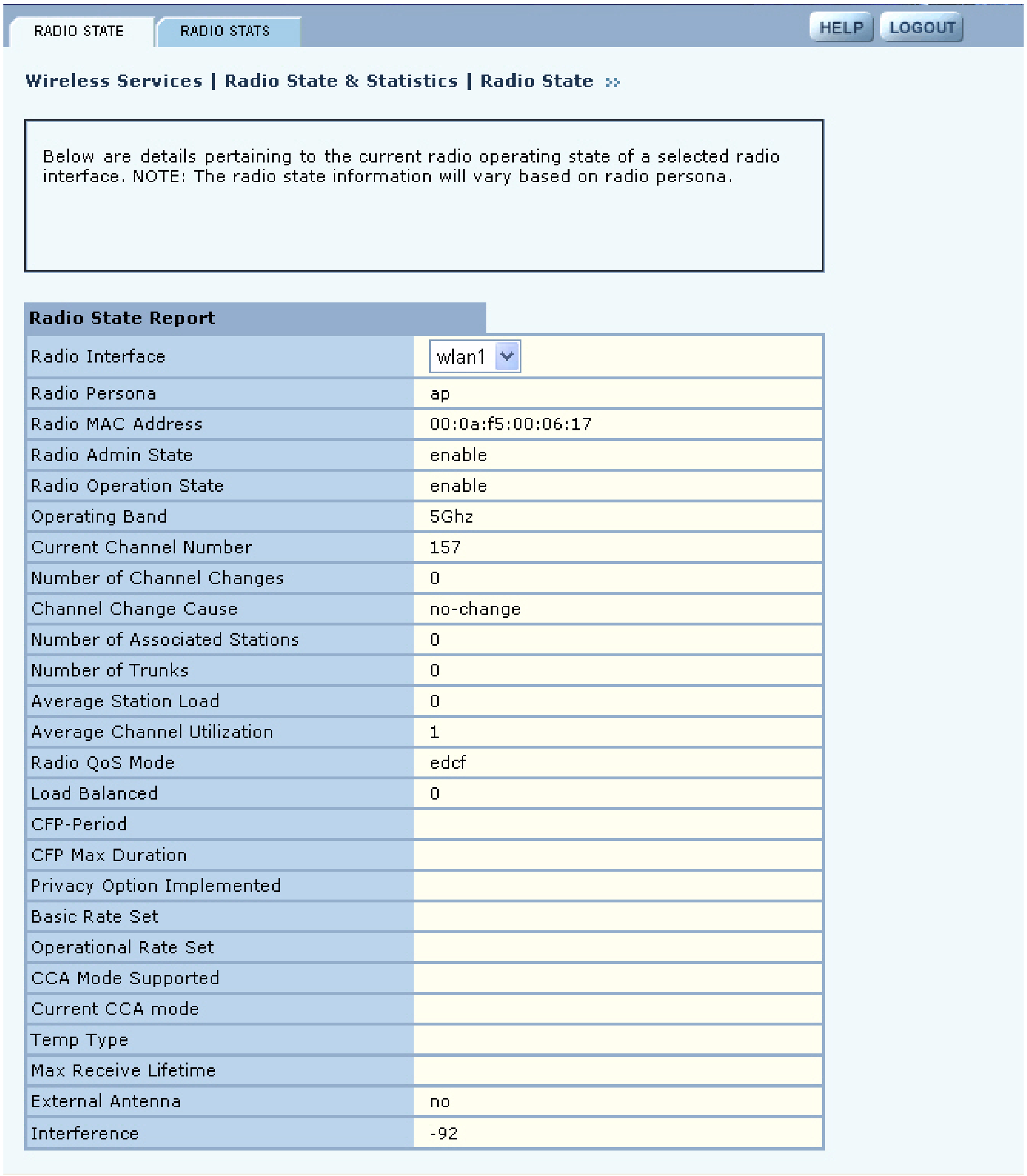
Select **Radio State & Statistics** from the Wireless Services menu to view the current state of each radio and the current communication statistics. This panel contains the following tabs:

- Radio State—View current configuration.
- Radio Statistics—View information about current operation.

Radio State

The Radio State tab (Figure 49) contains details on the current configuration and utilization of each radio interface. The state information varies according to whether the radio is operating as a normal access point radio (AP mode) or as a backhaul point (BP mode).

Figure 49: Radio State Tab



Wireless Services | Radio State & Statistics | Radio State

Below are details pertaining to the current radio operating state of a selected radio interface. NOTE: The radio state information will vary based on radio persona.

Radio State Report	
Radio Interface	wlan1
Radio Persona	ap
Radio MAC Address	00:0a:f5:00:06:17
Radio Admin State	enable
Radio Operation State	enable
Operating Band	5Ghz
Current Channel Number	157
Number of Channel Changes	0
Channel Change Cause	no-change
Number of Associated Stations	0
Number of Trunks	0
Average Station Load	0
Average Channel Utilization	1
Radio QoS Mode	edcf
Load Balanced	0
CFP-Period	
CFP Max Duration	
Privacy Option Implemented	
Basic Rate Set	
Operational Rate Set	
CCA Mode Supported	
Current CCA mode	
Temp Type	
Max Receive Lifetime	
External Antenna	no
Interference	-92

Use the pull-down list to switch between radios. This tab contains the following information:

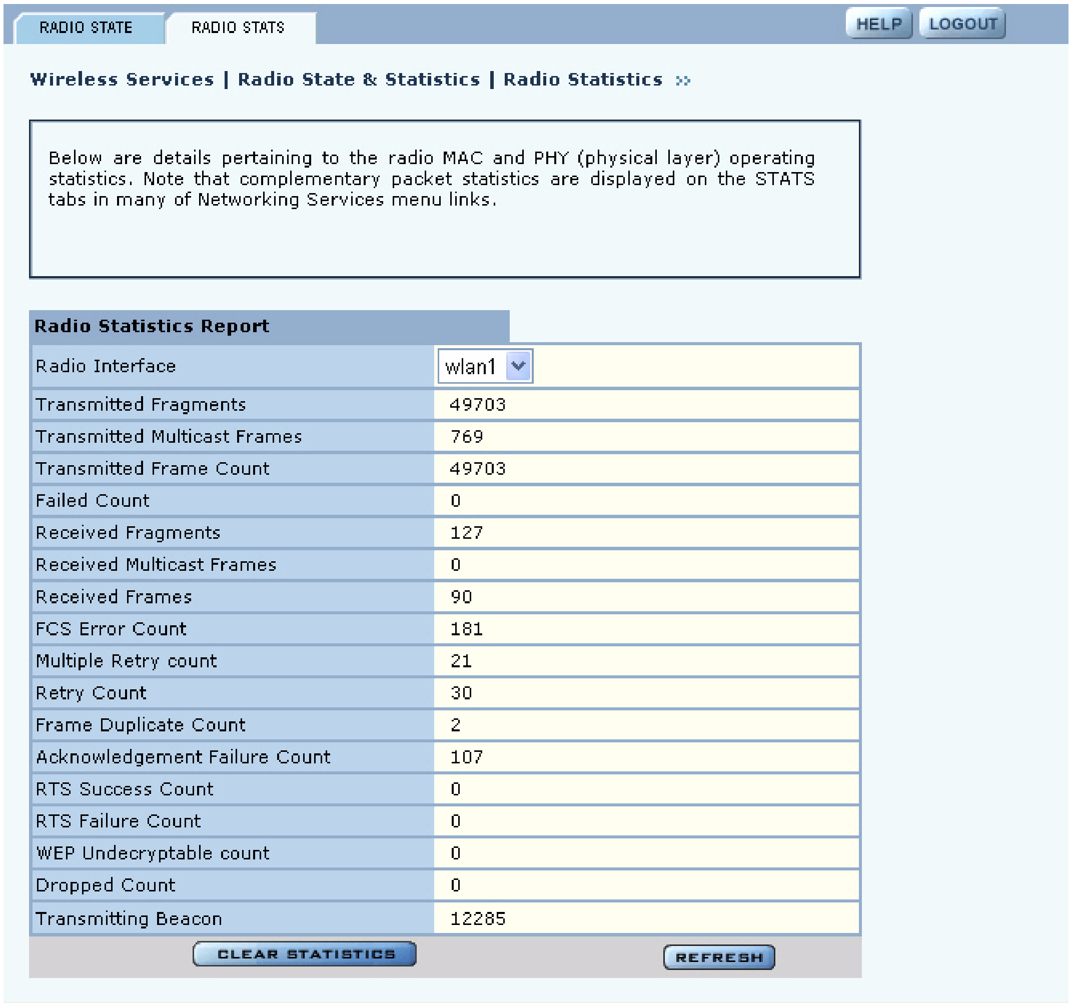
Field	Description
Radio Persona	Mode of the radio - AP or BP
Radio MAC Address	MAC address of radio
Radio Admin State	Administrative status of the radio (enabled or disabled)
Radio Operation State	Operational status of the radio (enabled or disabled)
Operating Band	Current band of operation

Field (continued)	Description
Current Channel Number	Current channel of operation
Number of channel changes	Number of times the channel has changed since boot-up (AP persona only)
Channel Change Cause	Reason the frequency changed since boot-up, if appropriate, due to user intervention or performance degradation (AP persona only)
Number of Associated Stations	The number of stations that are associated to the radio (AP persona only)
Number of trunks	Number of backhaul trunks associated with the radio (AP persona only)
Average Station Load	Average load on client stations in percent (AP persona only)
Average Channel Utilization	Average load on channels in percent (AP persona only)
Radio QoS Mode	Mode used for class of service mapping
Load Balanced	Number of stations that are load balanced (AP persona only)
CFP-Period	Number of DTIM intervals between the start of Contention Free Periods (CFPs).
CFP Max Duration	Maximum duration of the CFP in time units that may be generated by the AP.
Privacy Option Implemented	Security setting
Basic Rate Set	Set of basic rates for BSS (AP persona only)
Operational Rate Set	Set of operational rates for BSS
CCA mode supported	List of all of the Clear Channel Assessment (CCA) modes supported by the PHY
Current CCA mode	current CCA method in operation
Temp Type	Current physical operating temperature range capability.
Max Receive Lifetime	Maximum MSDU receive lifetime
External antenna	Indication of whether the radio has an external antenna (true) or not (false)
Interference	Radio interference in the surrounding wireless environment pertaining to the channel of operation, in dBm. (AP persona only)

Radio Statistics

The Radio Statistics tab (Figure 50) contains information on the operation of each radio. This information varies according to whether the radio is in the AP or BP persona. The statistics refresh every 10 seconds.

Figure 50: Radio Statistics Tab



Wireless Services | Radio State & Statistics | Radio Statistics »

Below are details pertaining to the radio MAC and PHY (physical layer) operating statistics. Note that complementary packet statistics are displayed on the STATS tabs in many of Networking Services menu links.

Radio Statistics Report

Radio Interface	wlan1
Transmitted Fragments	49703
Transmitted Multicast Frames	769
Transmitted Frame Count	49703
Failed Count	0
Received Fragments	127
Received Multicast Frames	0
Received Frames	90
FCS Error Count	181
Multiple Retry count	21
Retry Count	30
Frame Duplicate Count	2
Acknowledgement Failure Count	107
RTS Success Count	0
RTS Failure Count	0
WEP Undecryptable count	0
Dropped Count	0
Transmitting Beacon	12285

Use the pull-down list to switch between radios. This tab contains the following information:

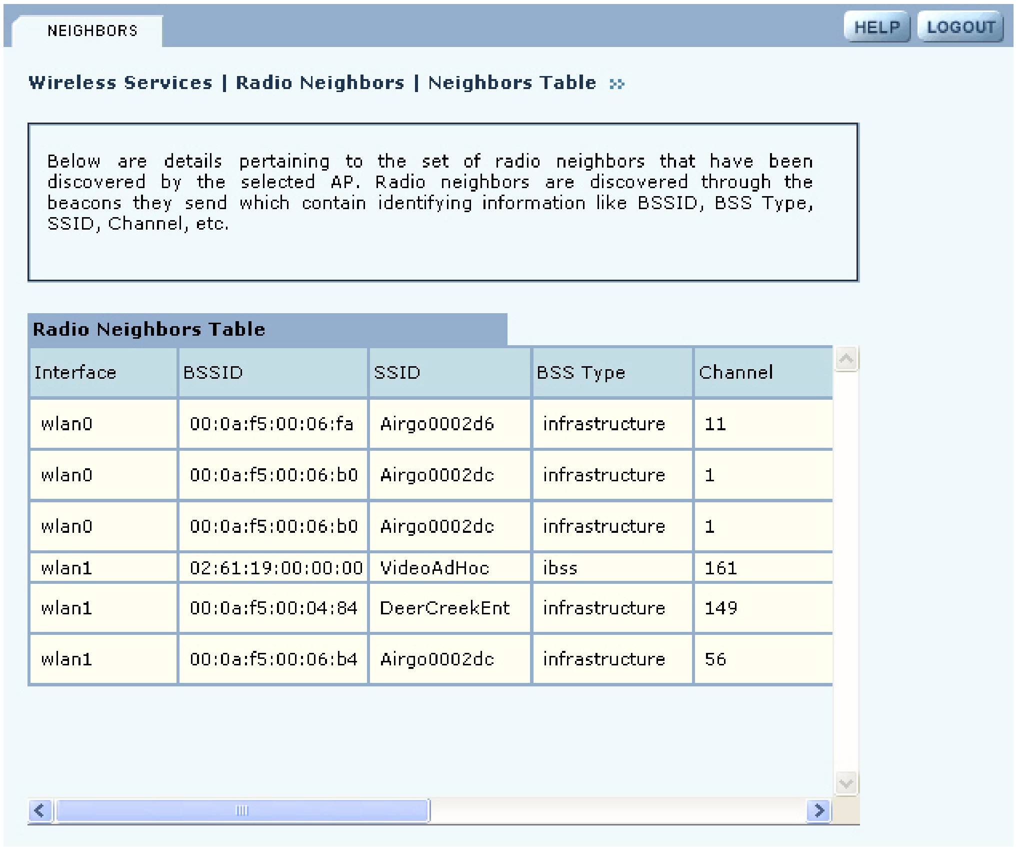
Field	Description
Transmitted Fragment Count	Number of transmitted fragments (MAC Protocol Data Units) that have been acknowledged since last power-up or last Clear Statistics request
Transmitted Multicast Frame Count	Number of transmitted multicast frames (MAC Service Data Units)
Failed Count	Count of MSDU not transmitted successfully due to the number of transmit attempts exceeding either the dot11ShortRetryLimit or dot11LongRetryLimit.
Received Fragment Count	Count for successfully received MPDUs of type Data or Management.
Received Frame Count	Count of successfully received frames (MSDUs)

Field (continued)	Description
FCS Error Count	Count of FCS errors detected when receiving a MPDU.
Received Multicast Frame Count	Count when a MSDU is received with the multicast bit set in the destination MAC address.
Multiple Retry Count	Count of successful transmissions after more than one retransmission.
Retry Count	Count of successful transmissions after one or more retransmission
Frame Duplicate Count	Count of frames received in which the Sequence Control field indicates it is a duplicate frame.
Ack Failure Count	Count of expected acks not received.
RTS Success Count	Count of successful CTS received in response to a RTS
RTS Fail Count	Count of RTS for which a CTS response is not received.
Transmitted Frame Count	Count for successfully transmitted MSDUs.
WEP Undecryptable Count	Number of times a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the Transmitter MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option. (Valid only if encryption is WEP)
# of transmitted Beacons	Count of successfully transmitted beacons

Viewing Radio Neighbor Details

A radio neighbor is a radio whose beacon frame is detected by the AP. Select **Radio Neighbors** from the Wireless Services menu to view summary information on all the neighboring APs within beacon range (Figure 51).

Figure 51: Radio Neighbors



Wireless Services | Radio Neighbors | Neighbors Table

Below are details pertaining to the set of radio neighbors that have been discovered by the selected AP. Radio neighbors are discovered through the beacons they send which contain identifying information like BSSID, BSS Type, SSID, Channel, etc.

Radio Neighbors Table

Interface	BSSID	SSID	BSS Type	Channel
wlan0	00:0a:f5:00:06:fa	Airgo0002d6	infrastructure	11
wlan0	00:0a:f5:00:06:b0	Airgo0002dc	infrastructure	1
wlan0	00:0a:f5:00:06:b0	Airgo0002dc	infrastructure	1
wlan1	02:61:19:00:00:00	VideoAdHoc	ibss	161
wlan1	00:0a:f5:00:04:84	DeerCreekEnt	infrastructure	149
wlan1	00:0a:f5:00:06:b4	Airgo0002dc	infrastructure	56

The summary table lists the following information:

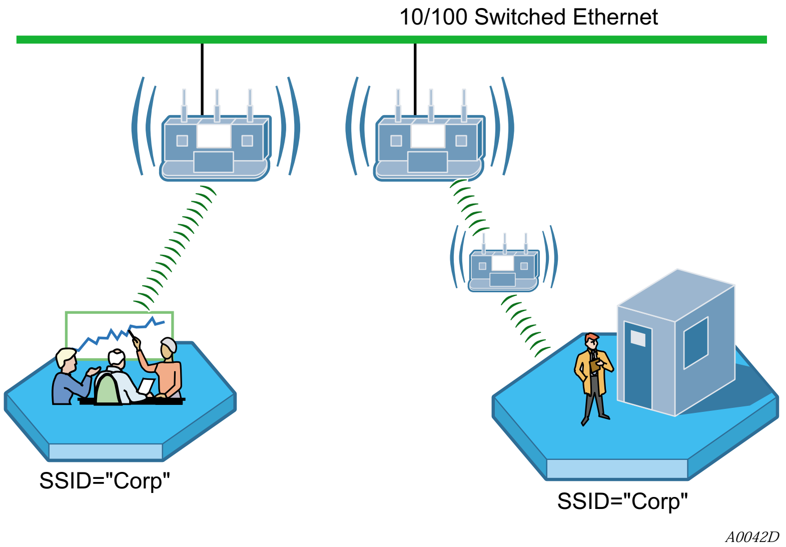
Field	Description
Interface	The AP radio (wlan0 or wlan1)
BSSID	The MAC address of the neighboring AP radio, which determines the BSS
SSID	The name of the network (ESS) in which the AP is operating
BSS Type	Infrastructure or ad-hoc network arrangement
Channel	Current channel of operation for the neighboring BSS
AP Beacon Name	Name of the neighboring AP in the beacon frame
Compatibility Status	Indication of whether or not the neighbor is an AP with which the IAPP protocol can be established
Strength	Strength of Radio neighbor signal, in percent
Load percentage	Load on the AP, in percent
STA Count	Number of client stations served by the neighboring AP

Use the scrolling bars to display the full range of interfaces and data.

Configuring SSID Parameters

A wireless network is formed when a set of APs advertises the same value as the SSID, or network name. Figure 52 shows the Acme Works network with multiple 108 Mbps Wireless APs, each advertising the same “Corporate” SSID.

Figure 52: Example “Corporate” Network



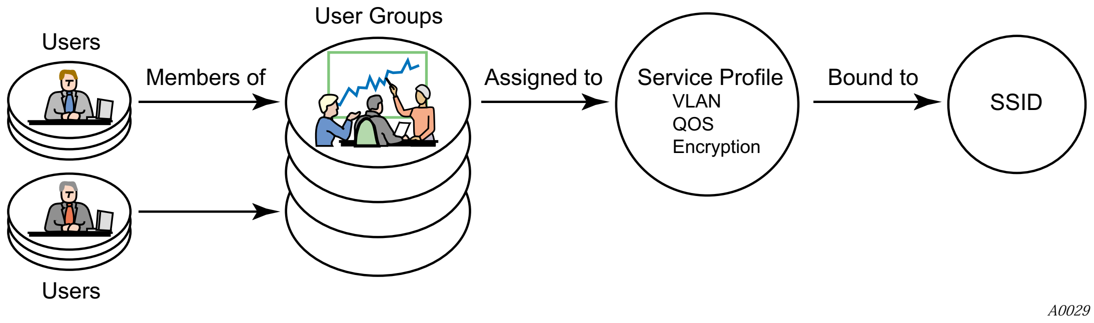
Each 108 Mbps Wireless AP is shipped with a default SSID, which must be replaced during the bootstrap process (see “Using AP Quick Start to Initialize the Access Point” on page 31) or from the SSID Configuration panel, as explained in this section. Multiple SSIDs are also supported. “Multiple SSIDs” on page 86 explains how to enable this feature and permit clients to access multiple wireless networks through the same access point.

SSIDs and Service Profiles

A service profile consists of VLAN, COS, and minimal security attributes applied to a network or to designated classes of users once they are authenticated by a RADIUS authentication server (security portal or external authentication server). If the service profile is defined without reference to a specific user group and bound to an SSID, then the profile is applied to all users who access the network.

Figure 53 illustrates the relationship between users, user groups, service profiles, and SSID. A RADIUS authentication server stores user group information and uses that information to match users to groups during authentication. Upon authentication, a previously-defined service profile is assigned to the user based on user group membership. The service profile, in turn, is bound to the SSID and thereby determines level of service awarded to the user.

Figure 53: SSIDs and Service Profiles



From the SSID Configuration panels, you can define service profiles for user groups and then bind the profiles to the SSID. A user who requests access to the network is authenticated and placed into the appropriate user group, and the AP software automatically applies the privileges and restrictions defined in the service profile for that group. Each user group can be assigned to just one service profile, but multiple groups can share the same service profile.

NOTE: The SSID settings in this section apply only to AP mode radios. The Backhaul Configuration panel described in “Configuring a Wireless Backhaul” on page 129 is used to configure the SSID for the BP radio. Make sure that the SSID configuration for the AP matches that of the other APs in the network.

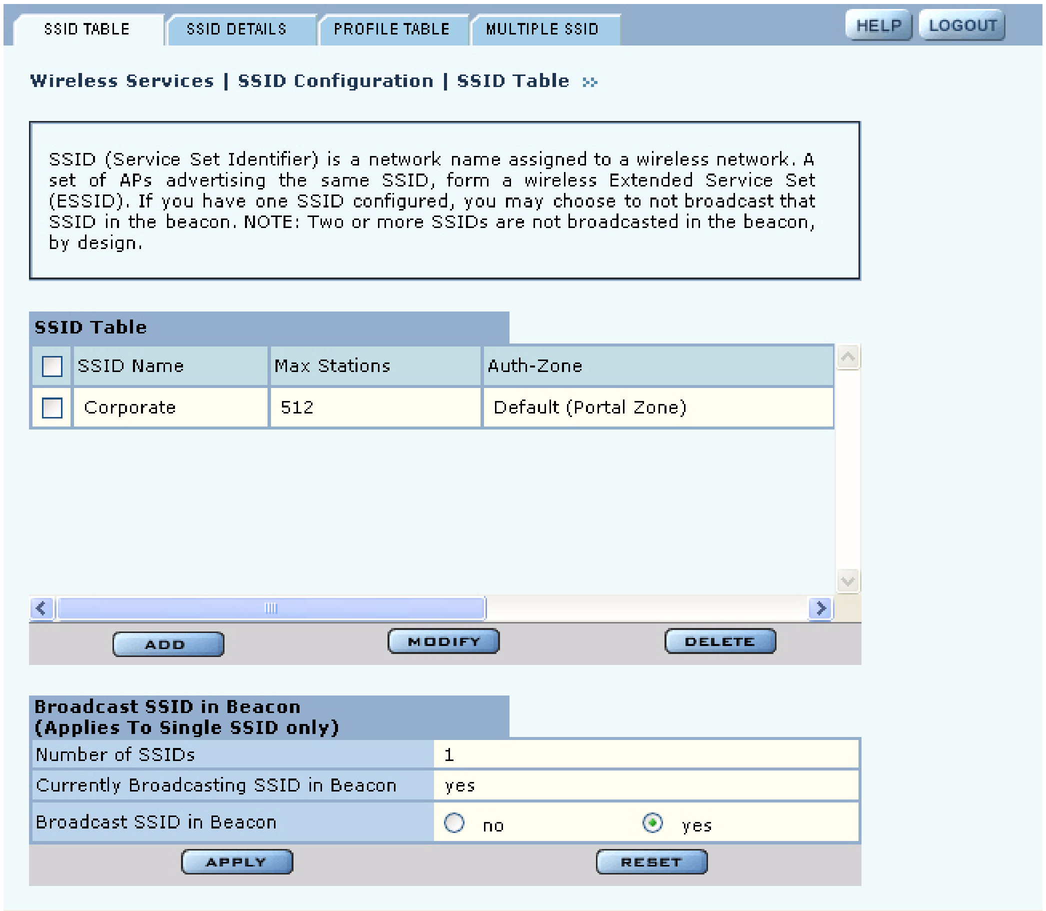
Select **SSID Configuration** from the Wireless Services menu to open the SSID Configuration panel. The panel contains the following tabs:

- SSID Table—View the current SSID configuration, modify the configuration, or add new SSIDs.
- SSID Details—View the association between SSIDs and service profiles.
- Profile Table—Manage service profiles.
- Multiple SSID—Enable the multiple SSID feature.

SSID Table

Select **SSID Configuration** from the Wireless Services menu to open the SSID Table (Figure 54).

Figure 54: SSID Configuration - SSID Table



Wireless Services | SSID Configuration | SSID Table »

SSID (Service Set Identifier) is a network name assigned to a wireless network. A set of APs advertising the same SSID, form a wireless Extended Service Set (ESSID). If you have one SSID configured, you may choose to not broadcast that SSID in the beacon. NOTE: Two or more SSIDs are not broadcasted in the beacon, by design.

SSID Table

□	SSID Name	Max Stations	Auth-Zone
□	Corporate	512	Default (Portal Zone)

Broadcast SSID in Beacon (Applies To Single SSID only)

Number of SSIDs	1
Currently Broadcasting SSID in Beacon	yes
Broadcast SSID in Beacon	○ no ● yes

The table lists the following information about each SSID:

Field	Description
SSID Name	Name (maximum 32 alphanumeric characters). This name is used only by the radio in AP mode, and is broadcast in its beacon. For a radio in backhaul point mode, the SSID name is entered in the Backhaul Configuration, Link Criteria tab (see Chapter 6).
Max stations	The maximum number of stations that can be associated to this SSID on this AP. The range is 1-512. If the maximum number of stations is reached and a new client tries to associate to the AP, the association attempt is rejected. Association is also rejected if the number of clients is less than the maximum but exceeds the number of client stations permitted by the AP license.
Auth Zone	The RADIUS authentication zone for the SSID
PSK-Type	The type of pre-shared key used, if WPA is the encryption suite
MAC-ACL	MAC-ACL authentication enabled or disabled
Auth Servers	The RADIUS server used for user authentication

Follow these steps to rename the SSID or modify its configuration:

1. Click **Modify** to open the SSID Details table, which also provides access to service profiles for the SSID.
2. Enter the new SSID name.
3. Click **Apply**. If an SSID is renamed, all configuration details related to the old SSID name, such as service profile associations and security configuration, are automatically transferred, and the radios that operate in AP mode now broadcast the new SSID in the beacon.

The default SSID cannot be modified. If an attempt is made to modify the default SSID, the system prompts you to first rename it. If you select the current SSID in the table and click **Delete**, the SSID reverts to the default.

The 108 Mbps Wireless AP can be configured to support multiple SSIDs. If this feature is enabled on the Multiple SSID tab ("Multiple SSIDs" on page 86), then it is possible to add new SSIDs from the SSID Table tab, in addition to modifying or deleting an existing SSID.

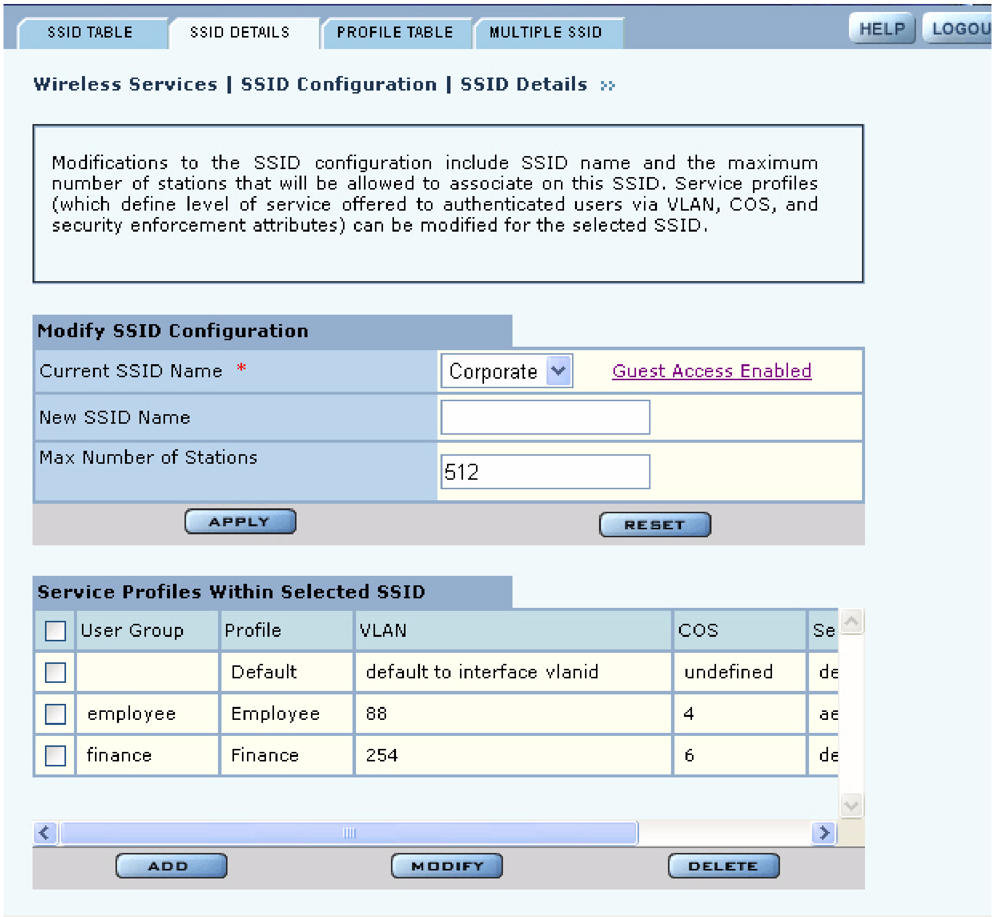
Perform the following functions on the SSID Table tab:

Function	Description
Add new SSID (if multiple SSID is enabled)	**1** Click **Add** and enter the following information: • SSID name—This name is used only by the radio in AP mode. For a radio in backhaul point mode, enter the SSID name in the Backhaul Configuration, Link Criteria tab (see Chapter 6). • Max Number of Stations—Enter a maximum number of clients stations, if desired. The range of values is 1-512. If the maximum number of stations is reached and a new client tries to associate to the AP, the association attempt is rejected. Association is also rejected if the number of clients is less than the maximum but exceeds the number of client stations permitted by the AP license. **2** Click **Apply**.
Modify an existing SSID	**1** Select the SSID and click **Modify** to open the SSID Details table, which also provides access to service profiles for the SSID. **2** Enter the new SSID name. **3** Confirm the maximum number of stations **4** Click **Apply**.
Delete an SSID (if multiple SSID is enabled)	Click **Delete**, and click **OK** to confirm.
Change the SSID broadcast setting (single SSID configurations only)	For single SSID configurations, the SSID Table tab provides the option to broadcast the SSID in the AP beacon, or to suppress broadcast of the SSID for increased security. The SSID is never broadcast in multiple SSID configurations. To change the SSID broadcast setting: **1** Select **no** or **yes**. **2** Click **Apply**.

SSID Details

Use the SSID Details Tab (Figure 55) to modify an SSID and bind service profiles to an SSID.

Figure 55: SSID Configuration - SSID Details



Wireless Services | SSID Configuration | SSID Details »

Modifications to the SSID configuration include SSID name and the maximum number of stations that will be allowed to associate on this SSID. Service profiles (which define level of service offered to authenticated users via VLAN, COS, and security enforcement attributes) can be modified for the selected SSID.

Modify SSID Configuration

Current SSID Name *	Corporate	Guest Access Enabled
New SSID Name		
Max Number of Stations	512	

Service Profiles Within Selected SSID

□	User Group	Profile	VLAN	COS	Se
□		Default	default to interface vlanid	undefined	de
□	employee	Employee	88	4	ae
□	finance	Finance	254	6	de

The tab contains two areas. Use the Modify SSID Configuration area to change the current SSID configuration, as described in “SSID Table” on page 81. The bottom area shows the service profiles currently bound to the SSID. This list includes the following information for each service profile:

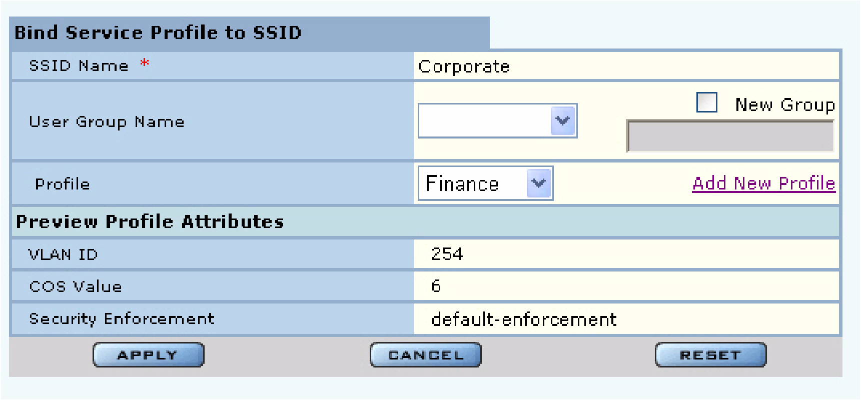
Feature	Description
User Group	User group linked to the service profile. If this entry is empty, the user group is null. The null user group is automatically assigned to the default service profile, unless it is explicitly bound to another service profile. RADIUS authentication must be active in order for user groups to be effective. The user group for a given client is passed to the AP as a RADIUS attribute for each successfully-authenticated user. To edit the group information, click the group name link. Any attempt to delete the null user group, automatically associates it to the default service profile.
Profile	Service profile name.
VLAN	VLAN assigned to the service profile.
COS	Class of service values assigned to the service profile.

Feature (continued)	Description
Security Enforcement	Type of encryption required for the service profile. For user groups assigned to this service profile, the security enforcement setting supersedes the encryption type configured for the overall network.

Perform the following functions from the service profile list on this tab:

Function	Steps
Bind an existing service profile to an SSID	**1** Click **Add** to open the Bind Service Profile to SSID entry panel (Figure 56). **2** Select the profile name, or click **Add New Profile** to create a new profile according to the instructions in “Profile Table” on page 85. **3** Select a group name from the existing RADIUS group names to associate with the profile, or select **New Group** and enter a new user group name. **4** Click **Apply**.
Change service profile binding	**1** Select the checkbox for the user group and profile, and click **Modify** to open the Bind Service Profile to SSID entry panel (Figure 56) in modify mode. **2** Select a profile to bind to the SSID, or click **Add New Profile** to create a new profile according to the instructions in “Profile Table” on page 85. **3** Click **Apply**.
Delete service profile binding	**1** Select the checkbox for the user group and profile, and click **Delete**. **2** Click **OK** to confirm.
Configure security for the SSID	Click **Go** at the bottom of the panel. The button leads to the SSID Authentication tab of the Wireless Security panel. For instructions on defining the security settings, refer to “SSID Authentication” on page 142. After defining the security settings, click **Back** on the browser to return to the SSID Details tab.

Figure 56: SSID Configuration - Bind Service Profile to SSID



Bind Service Profile to SSID

SSID Name *	Corporate
User Group Name	☐ New Group
Profile	Finance

Preview Profile Attributes

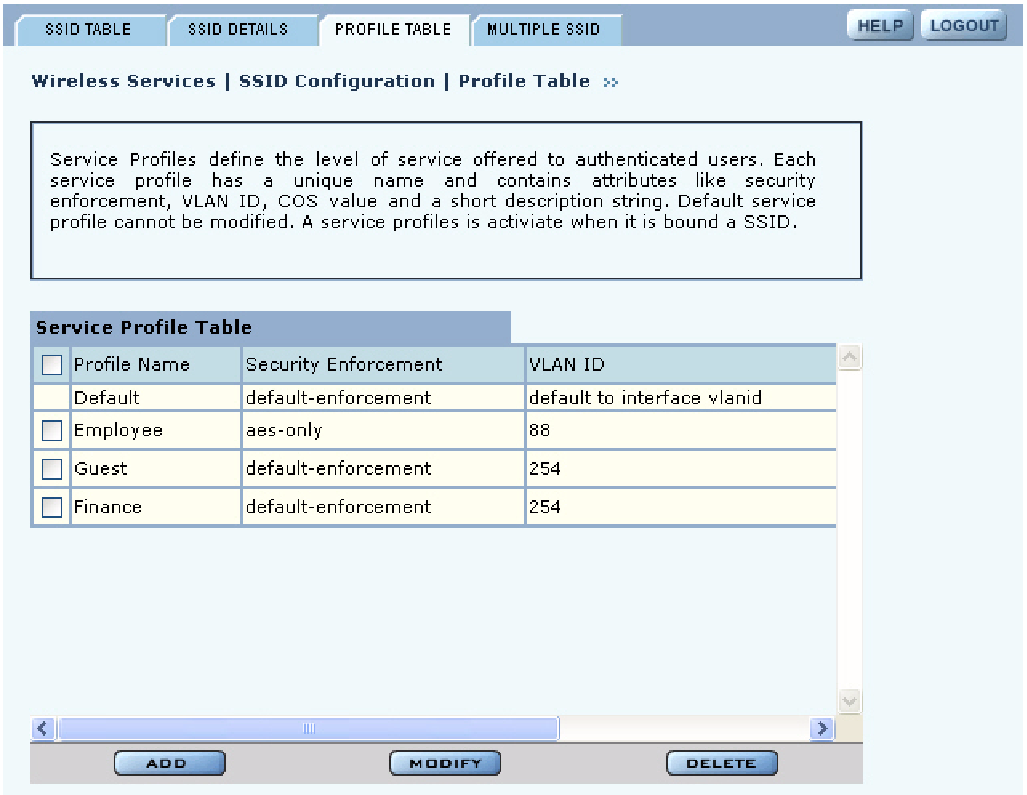
VLAN ID	254
COS Value	6
Security Enforcement	default-enforcement

Profile Table

The Profile Table tab (Figure 57) lists all the currently defined service profiles. Each service profile includes attributes for security enforcement, VLAN ID, and COS value. Binding a service profile to an SSID determines the privileges and restrictions that apply to user groups associated with the profile.

NOTE: Changes made to SSID or service profiles cause affected users to be automatically disassociated from the AP. The AP then attempts to reassociate them automatically. This causes a momentary interruption in service.

Figure 57: SSID Configuration - Profile Table



Service Profiles define the level of service offered to authenticated users. Each service profile has a unique name and contains attributes like security enforcement, VLAN ID, COS value and a short description string. Default service profile cannot be modified. A service profiles is activiate when it is bound a SSID.

Service Profile Table

□	Profile Name	Security Enforcement	VLAN ID
	Default	default-enforcement	default to interface vlanid
□	Employee	aes-only	88
□	Guest	default-enforcement	254
□	Finance	default-enforcement	254

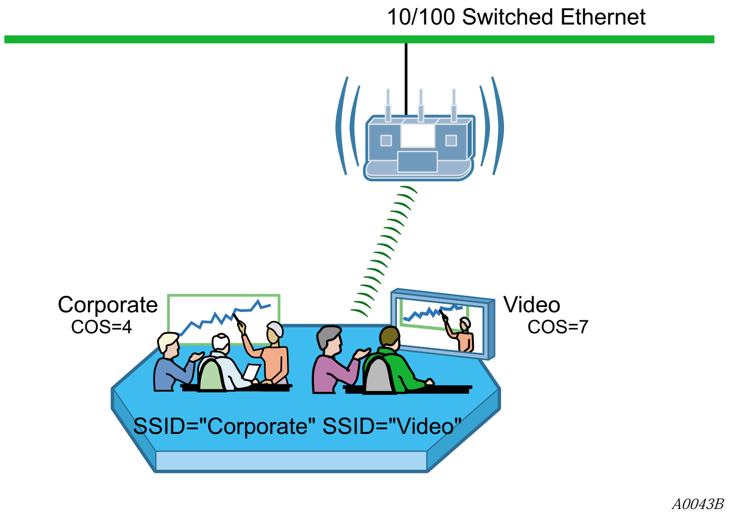
Perform the following functions from this tab:

Function	Steps
Add a new service profile	**1** Click **Add** to create a new service profile. **2** Enter the profile name, which must be unique. (required) **3** Select the VLAN for the profile. **4** Enter a COS value for the profile. The range is 0-7. For more information, see “Configuring Quality of Service” on page 113. **5** Select an enforcement level for data encryption to apply to the profile. This setting provides fine-grained security options at the user group level. Default-enforcement refers to the encryption settings that prevail in the network at large. The security enforcement applies after authentication is complete. **6** Enter a description, if desired. **7** Click **Apply** to save the profile or **Cancel** to return to the Profile Table.
Modify a profile	**1** Select the profile from the table and click **Modify**. **2** Make changes as desired, and click **Apply**, or click **Cancel** to return to the Profile Table without saving changes. User groups bound to the profile automatically inherit any modified attributes. It is not possible to modify the default profile.
Delete a profile	A service profile can only be deleted if there are no groups under the SSID bound to the profile. It is not possible to delete the default profile.

Multiple SSIDs

With the multiple SSID feature, the same physical network infrastructure can support multiple wireless networks. Each network (identified by SSID) can have its own service profile and associated level of service. For example, Figure 58 shows how Acme Works configured two SSIDs: one to accommodate the normal corporate network and one for a separate video conference network, which requires a higher quality of service.

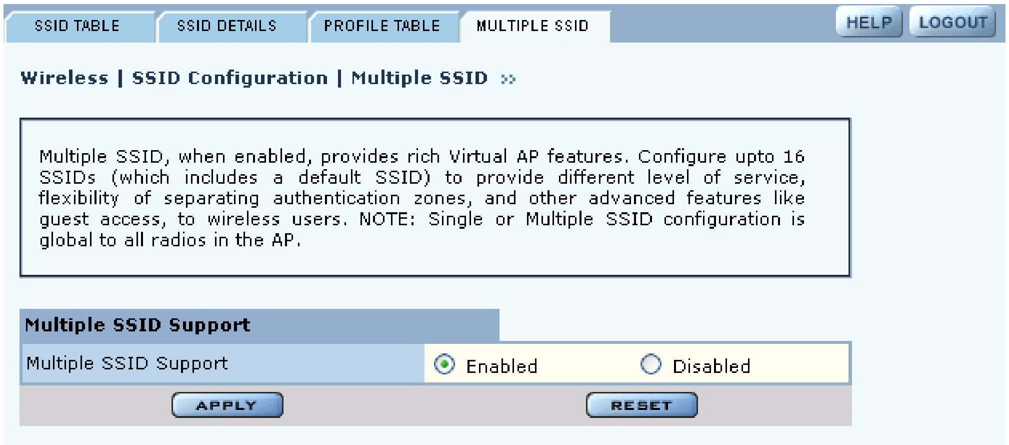
Figure 58: Example Use of Multiple SSIDs to Differentiate Levels of Service



Use the Multiple SSID tab (Figure 59) to enable the multiple SSID feature. Make a selection, and click **Apply**. After enabling the multiple SSID feature, additional SSIDs can be added on the SSID Table (see "SSID Table" on page 81).

When multiple SSIDs are enabled on the 108 Mbps Wireless AP, that AP no longer broadcasts an SSID in its beacon frame. In order for a client to associate with the 108 Mbps Wireless AP configured for multiple SSIDs, a profile for each target SSID must be created on the client workstation using the Windows Zero Config (WZC) Add function or the PLANEX Client Utility Create function.

Figure 59: SSID Configuration - Multiple SSID



Multiple SSID, when enabled, provides rich Virtual AP features. Configure upto 16 SSIDs (which includes a default SSID) to provide different level of service, flexibility of separating authentication zones, and other advanced features like guest access, to wireless users. NOTE: Single or Multiple SSID configuration is global to all radios in the AP.

Multiple SSID Support

Multiple SSID Support ● Enabled ○ Disabled

Managing Client Stations

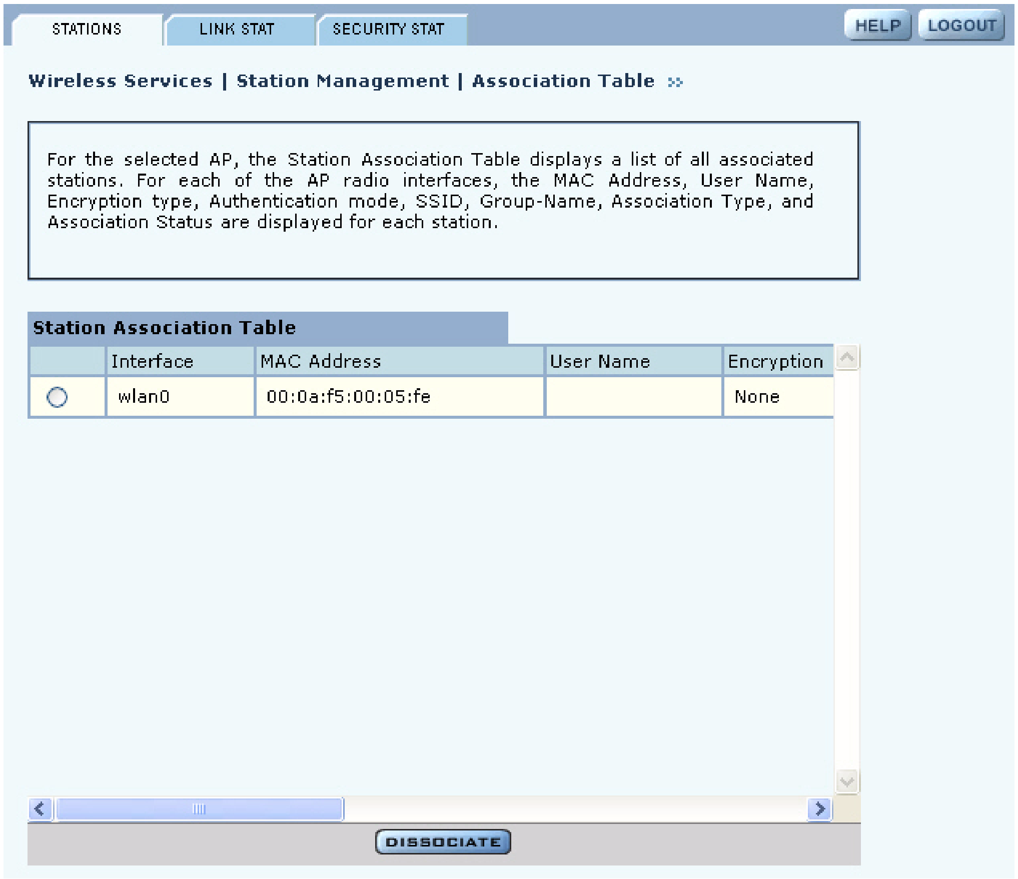
Select **Station Management** from the Wireless Services menu to open the Station Associations panel. The panel contains the following tabs:

- Stations—View all client stations associated to this 108 Mbps Wireless AP.
- Link Stat—View signal strength, signal quality and all the MAC level statistics.
- Security Stat—View 802.1x security statistics.

Stations

The Stations tab (Figure 60) shows the client stations that are currently associated to the AP.

Figure 60: Station Management - Stations


STATIONS
LINK STAT
SECURITY STAT
HELP
LOGOUT
Wireless Services | Station Management | Association Table »
DISSOCIATE

For the selected AP, the Station Association Table displays a list of all associated stations. For each of the AP radio interfaces, the MAC Address, User Name, Encryption type, Authentication mode, SSID, Group-Name, Association Type, and Association Status are displayed for each station.

Station Association Table

	Interface	MAC Address	User Name	Encryption
○	wlan0	00:0a:f5:00:05:fe		None

Use this panel to control association to the 108 Mbps Wireless AP. The panel lists the following information for each client station associated to the AP:

Field	**Description**
Interface	The AP radio (wlan0, wlan1)
MAC address	MAC address of the client station
User Name	User name assigned through the RADIUS server. If MAC ACL is used, then the user name is the MAC address of the client station
Encryption	Type of encryption used by client station (AES, TKIP, WEP or no encryption)
Authentication	Type of authentication used by the client station (Open, Shared Key, EAP or MAC-ACL)
SSID	SSID to which the client station is associated
Group name	Group to which the client station belongs
Association Type	Normal or transferred. Transferred means that the client station has been moved from the mate AP radio.
Association Status	Associated or Reassociated to the AP

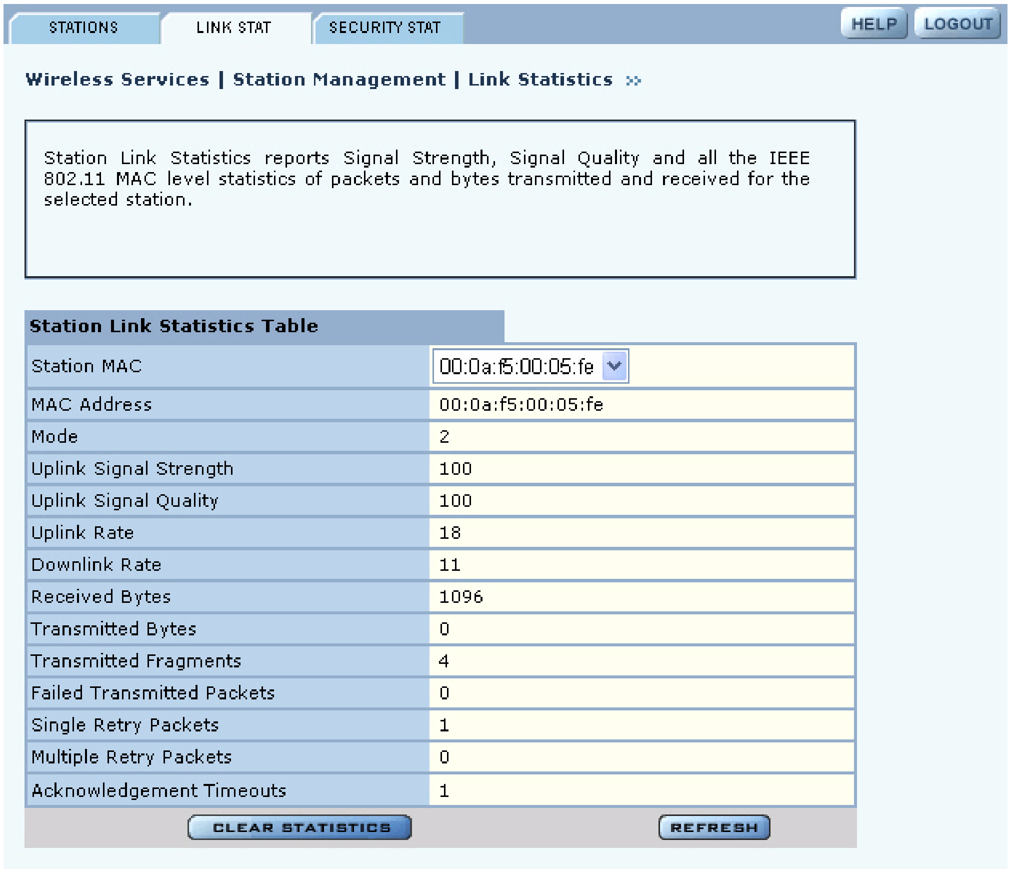
Select a station from the list and click a button at the bottom of the panel to perform any of the following functions:

Item	Description
Disassociate	Detach the station from the AP and remove station related information.
Link Stats	Display information about the link strength and quality between the AP and station
Security Stats	Display current security statistics

Link Statistics

The Link Stats table (Figure 61) provides details on the signal quality and strength between the AP and client station.

Figure 61: Station Link Statistics



Wireless Services | Station Management | Link Statistics »

Station Link Statistics reports Signal Strength, Signal Quality and all the IEEE 802.11 MAC level statistics of packets and bytes transmitted and received for the selected station.

Station Link Statistics Table	
Station MAC	00:0a:f5:00:05:fe
MAC Address	00:0a:f5:00:05:fe
Mode	2
Uplink Signal Strength	100
Uplink Signal Quality	100
Uplink Rate	18
Downlink Rate	11
Received Bytes	1096
Transmitted Bytes	0
Transmitted Fragments	4
Failed Transmitted Packets	0
Single Retry Packets	1
Multiple Retry Packets	0
Acknowledgement Timeouts	1

Select a station from the Station Associations table and click **Link Stats** to display the following information:

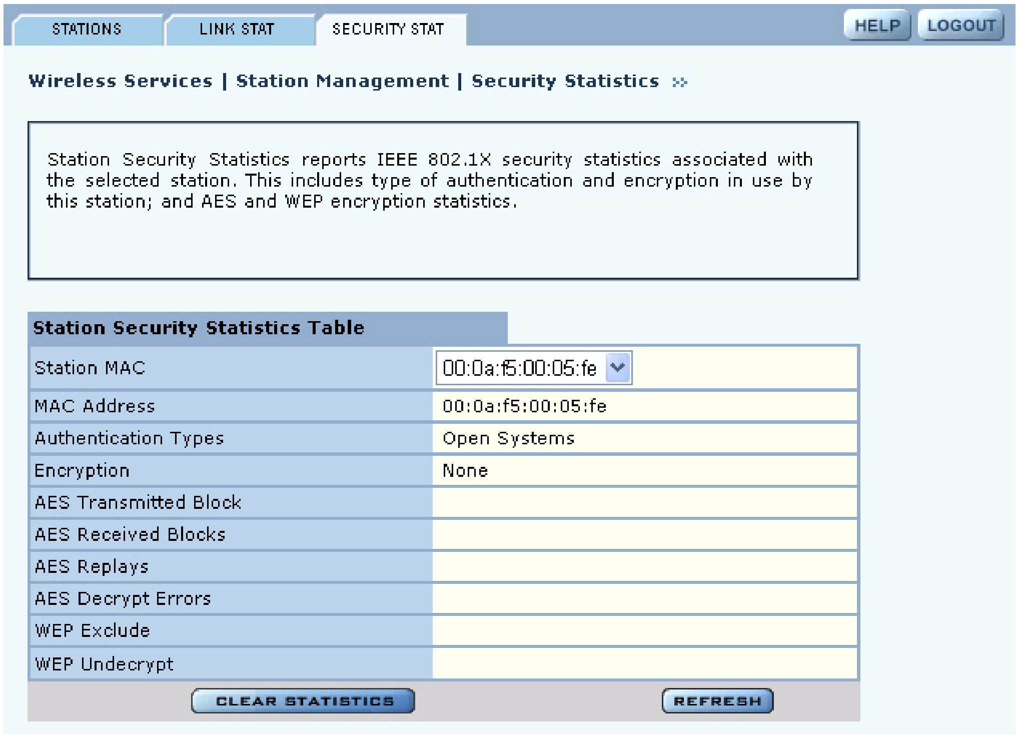
Field	Description
Station MAC address	The MAC address that identifies the station
Mode	802.11 mode used by the station (11a, 11b or 11g)
Uplink Signal Strength	Average signal strength on uplink (station to AP direction) as a percentage

Field (continued)	**Description**
Uplink Signal Quality	Average signal quality on uplink (station to AP direction) as a percentage
Uplink Rate	Average uplink data rate on uplink (Mbps)
Downlink rate	Average downlink data rate on uplink (Mbps
Received Bytes	Bytes received from the station
Transmitted Bytes	Bytes transmitted to station
Transmitted Fragments	Count of transmitted MPDUs
Failed Transmitted Packets	Number of MSDUs that were not transmitted successfully since retries exceeded short or long retry limit
Single Retry Packets	Number of packets that were successfully transmitted after one retry
Multiple Retry Packets	Number of packets that were successfully transmitted after multiple retries
Acknowledgement Timeouts	Number of packets that did not receive expected acknowledgement

Security Statistics

The Security Stats table (Figure 62) provides detailed security information for the connection between the AP and client station.

Figure 62: Station Security Statistics



STATIONS
LINK STAT
SECURITY STAT
HELP
LOGOUT
Wireless Services | Station Management | Security Statistics »

Station Security Statistics reports IEEE 802.1X security statistics associated with the selected station. This includes type of authentication and encryption in use by this station; and AES and WEP encryption statistics.

Station Security Statistics Table

Station MAC	00:0a:f5:00:05:fe
MAC Address	00:0a:f5:00:05:fe
Authentication Types	Open Systems
Encryption	None
AES Transmitted Block	
AES Received Blocks	
AES Replays	
AES Decrypt Errors	
WEP Exclude	
WEP Undecrypt	

Select a station from the Station Associations table and click **Security-Stats** to display the following information:

Field	Description
Station MAC address	The MAC address that identifies the station
Auth Type	Authentication used by station (Open, Shared key, EAP or MAC-ACL)
Encryption	Encryption used by station (AES, TKIP, WEP, or open access)
AES Transmitted Blocks	Number of AES transmitted blocks. Valid only if encryption is AES
AES Received blocks	Number of AES received blocks. Valid only if encryption is AES
AES Replays	Number of AES replays. Valid only if encryption is AES
AES Decrypt Errors	Number of AES decryption errors. Valid only if encryption is AES
WEP Excluded Count	Number of WEP exclude packets Valid only if encryption is WEP
WEP Undecryptable Count	Number of times frames were not encrypted or a frame was discarded due to the receiving station not implementing the privacy option. (Valid only if encryption is WEP.)

Configuring Inter Access Point Protocol (IAPP)

Inter-Access Point Protocol enables neighboring access points to keep up-to-date information concerning the status of roaming client stations. Select **IAPP Configuration** from the Wireless Services menu to configure the IAPP settings and to view the associated topology and statistics.

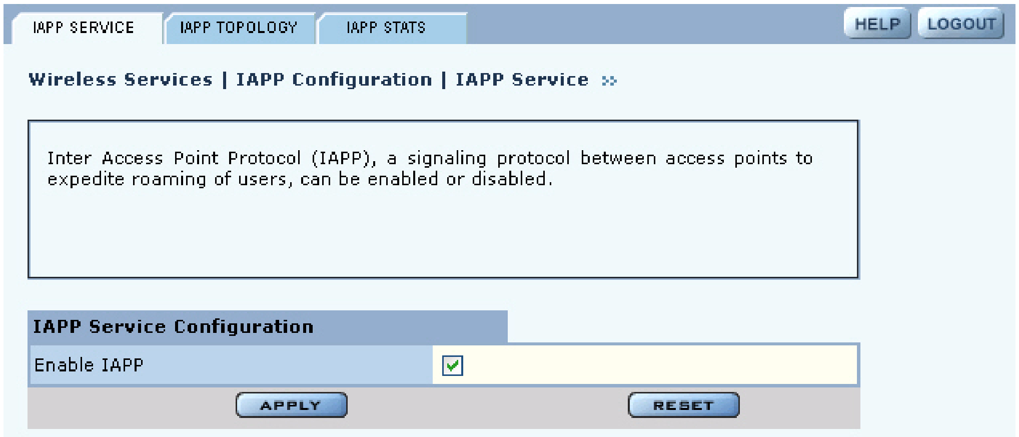
The panel contains the following tabs:

- IAPP Service—Enable or disable IAPP.
- Topology—View BSSID, IP address, and compatibility details.
- Stats—View statistics details, including notifications sent and received, “move” notification and response details, and details on Intra-AP moves.

IAPP Service

Use the IAPP Service tab (Figure 63) to enable IAPP. Selecting **Enable** initializes IAPP to perform network discovery and communicate with other APs. Click **Apply** to save changes.

Figure 63: IAPP Configuration - IAPP Service



Inter Access Point Protocol (IAPP), a signaling protocol between access points to expedite roaming of users, can be enabled or disabled.

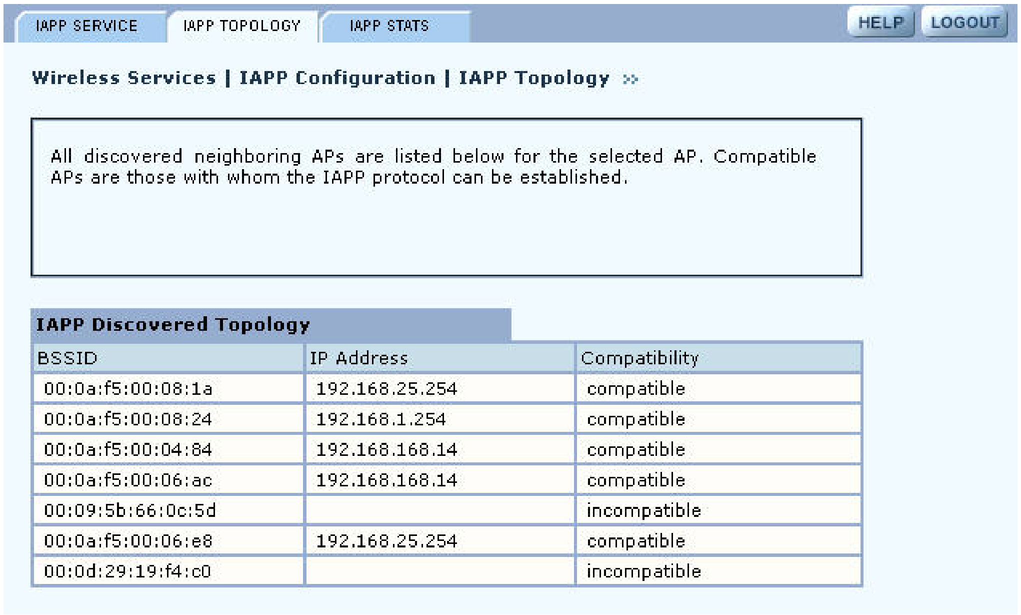
IAPP Service Configuration

Enable IAPP ☑

IAPP Topology

The read-only IAPP Topology tab (Figure 64) displays information about all the neighboring APs this AP has discovered, including the BSSID, IP address, and Compatibility (whether the IAPP protocol can be established with the neighboring AP).

Figure 64: IAPP Configuration - IAPP Topology



All discovered neighboring APs are listed below for the selected AP. Compatible APs are those with whom the IAPP protocol can be established.

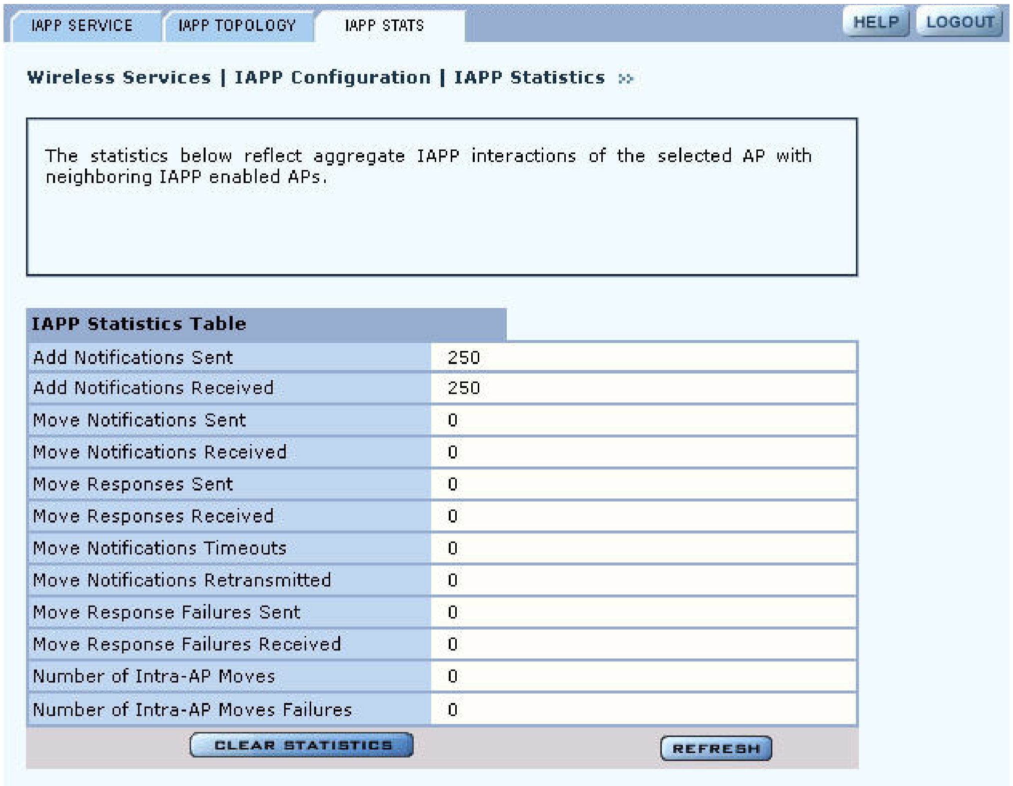
IAPP Discovered Topology

BSSID	IP Address	Compatibility
00:0a:f5:00:08:1a	192.168.25.254	compatible
00:0a:f5:00:08:24	192.168.1.254	compatible
00:0a:f5:00:04:84	192.168.168.14	compatible
00:0a:f5:00:06:ac	192.168.168.14	compatible
00:09:5b:66:0c:5d		incompatible
00:0a:f5:00:06:e8	192.168.25.254	compatible
00:0d:29:19:f4:c0		incompatible

IAPP Statistics

The IAPP Stats tab (Figure 65) lists information about IAPP activity.

Figure 65: IAPP Configuration - IAPP Stats



The statistics below reflect aggregate IAPP interactions of the selected AP with neighboring IAPP enabled APs.

IAPP Statistics Table	
Add Notifications Sent	250
Add Notifications Received	250
Move Notifications Sent	0
Move Notifications Received	0
Move Responses Sent	0
Move Responses Received	0
Move Notifications Timeouts	0
Move Notifications Retransmitted	0
Move Response Failures Sent	0
Move Response Failures Received	0
Number of Intra-AP Moves	0
Number of Intra-AP Moves Failures	0

This tab contains the following information:

Item	Description
Add Notifications Sent	Number of add-notifications sent to other APs in the local multicast domain due to stations associating to the AP
Add Notifications Received	Number of add-notifications received by the AP due to stations associating with other APs in the local multicast domain
Move Notifications Sent	Number of move notifications sent to other APs where the stations were previously associated
Move Notifications Received	Number of move notifications received from other APs to which the stations are currently associated
Move Responses Sent	Number of move responses sent to other APs when stations have reassociated with the other APs
Move Responses Received	Number of move responses received from other APs in the process of stations reassociating with this AP
Move Notifications Timeouts	Number of move notifications which were not sent in the maximum time allowed for a move transaction
Move Notifications Retransmitted	Number of times the move notifications were retransmitted for all the move transactions (not supported)

Item	Description
Move Response Failures Sent	Number of move responses with a FAILURE status sent to other APs during the station reassociating process
Move Response Failures Received	Number of move responses with a FAILURE status received from other APs during the station reassociating process
Number of Intra-AP Moves	Number of successful station reassociations between APs
Number of Intra-AP Moves Failures	Number of unsuccessful station reassociations between APs

Click **Clear Statistics** to return the statistics to zero and begin re-collecting them, and click **Refresh** to update the display with the most current information.

Performing Radio Diagnostics

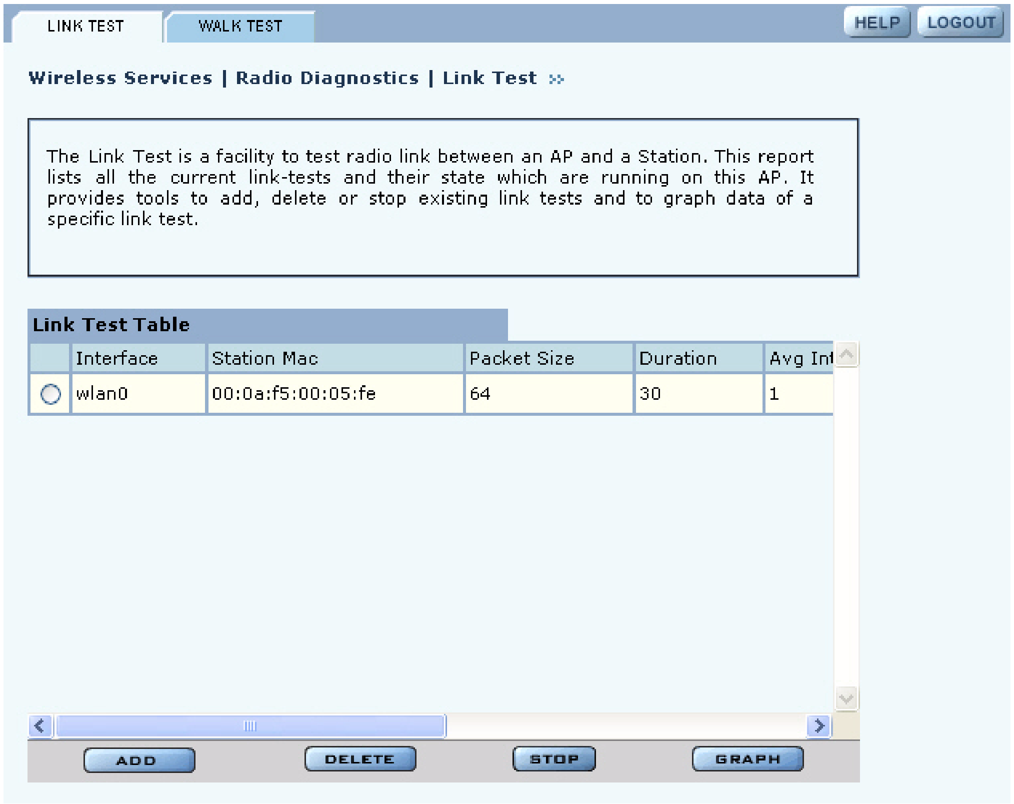
Choose **Radio Diagnostics** from the Wireless Services menu to test the radio signal between the AP and a client station. The panel contains 2 tabs:

- Link Test—Test the radio link between the AP and a client station.
- Walk Test—Advanced parameters regarding rate and range performance testing.

Link Test

Use the Link Test tab (Figure 66) to test connections to IP devices or run performance tests on specified links.

Figure 66: Radio Diagnostics - Link Test



Wireless Services | Radio Diagnostics | Link Test

The Link Test is a facility to test radio link between an AP and a Station. This report lists all the current link-tests and their state which are running on this AP. It provides tools to add, delete or stop existing link tests and to graph data of a specific link test.

Link Test Table

	Interface	Station Mac	Packet Size	Duration	Avg Int
○	wlan0	00:0a:f5:00:05:fe	64	30	1

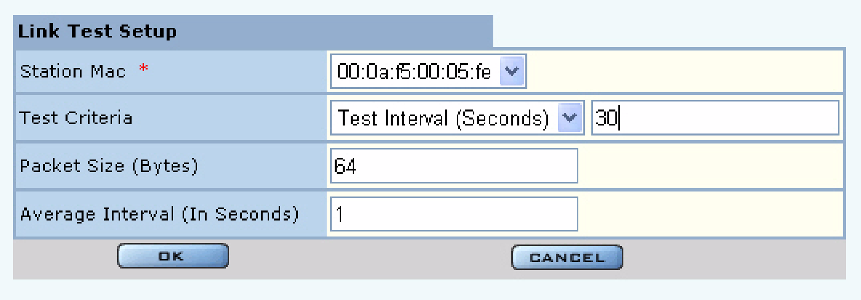
The Link Test tab includes the following information for each defined link test:

Field	Description
Interface	Select the AP radio
Station MAC	Select the MAC address of the station included in the link test
Packet Size	Specify the size of each link packet (in bytes)
Duration	Period during which the which the test runs
Average Interval	Sampling interval
Status	Current status of the link test. Click the Link Test tab to refresh

To perform a link test:

1 Click **Add** to open the Link Test Setup entry panel (Figure 66).

Figure 67: Radio Diagnostics - Link Test - Setup



Link Test Setup

Station Mac *	00:0a:f5:00:05:fe
Test Criteria	Test Interval (Seconds) 30
Packet Size (Bytes)	64
Average Interval (In Seconds)	1

2 Configure the following:

Field	Description
Interface	Select the AP radio
Station MAC Address	Select the MAC address of the station included in the link test
Test Criteria	Select whether the test is for a specified duration (seconds) or number of packets. Enter the duration in the area to the right of the Test Criteria pull-down list.
Packet Size	Specify the size of each link packet (in bytes)
Average Interval	Enter the interval over which link test data such as signal strength or signal quality is averaged

3 Click **OK** to save the test.

To confirm that the test is running, click **Link Test** to return to the Link Test table. Scroll the table columns to the right to view the Status column. When the test begins, the column displays the message: `Link Test Active`. Continue to refresh the display until you see the message: Link Test Completed Successfully.

Other recommendations for running a link test:

- Set the test duration to be greater than 5 minutes (or equivalent number of packets, for example 5 minutes = 1200 packets), and set the averaging interval greater than 30 seconds. This compensates for any momentary glitches in the wireless link.
- Generate traffic (such as ping traffic) to the station when performing the link test. If rate adaptation is active, this helps the uplink and downlink data rates settle at the maximum sustainable rates for that link.

A maximum of 10 link tests can be active on an AP at one time. The collected link test data is retained even after the link test is retained until manually deleted.

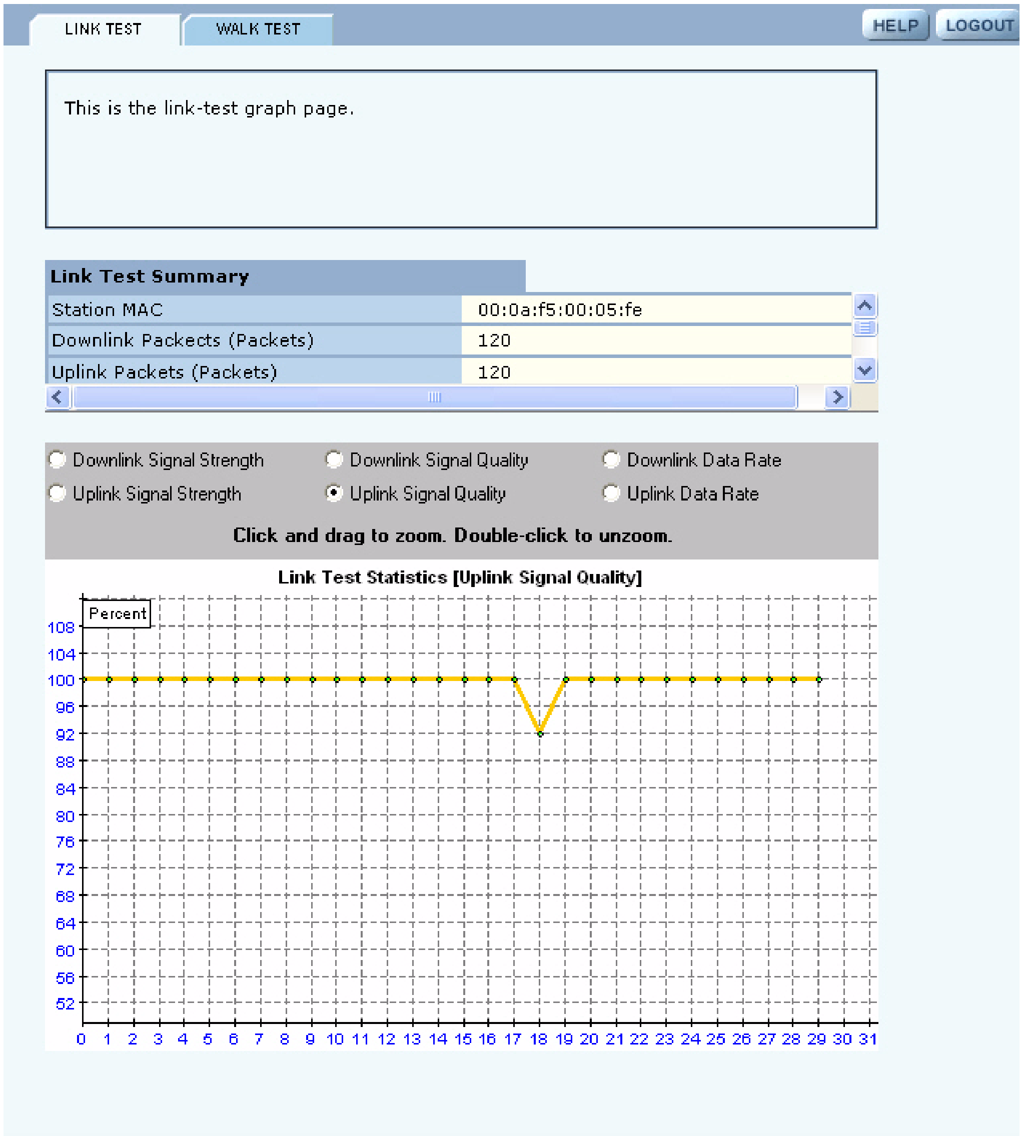
To graph the results of a link test, select the test on the Link Test tab, and click **Graph**. The Graph panel (Figure 68) opens.

Select from the following set of link test parameters to display a graph of the test results:

Item	Description
Downlink signal strength	Strength of the signal sent from the AP to the client station (percentage).
Uplink signal strength	Strength of the signal sent from the client station to the AP (percentage).
Downlink signal quality	Quality of the signal sent from the AP to the client station (percentage).
Uplink signal quality	Quality of the signal sent from the client station to the AP (percentage).
Downlink data rate	Transmission rate from the AP to the client station (Mbps).
Uplink data rate	Transmission rate from the client station to the AP (Mbps).

When a parameter is selected, that graph is displayed.

Figure 68: Radio Diagnostics - Link Test - Graph



This is the link-test graph page.

Link Test Summary

Station MAC	00:0a:f5:00:05:fe
Downlink Packects (Packets)	120
Uplink Packets (Packets)	120

○ Downlink Signal Strength ○ Downlink Signal Quality ○ Downlink Data Rate

○ Uplink Signal Strength ● Uplink Signal Quality ○ Uplink Data Rate

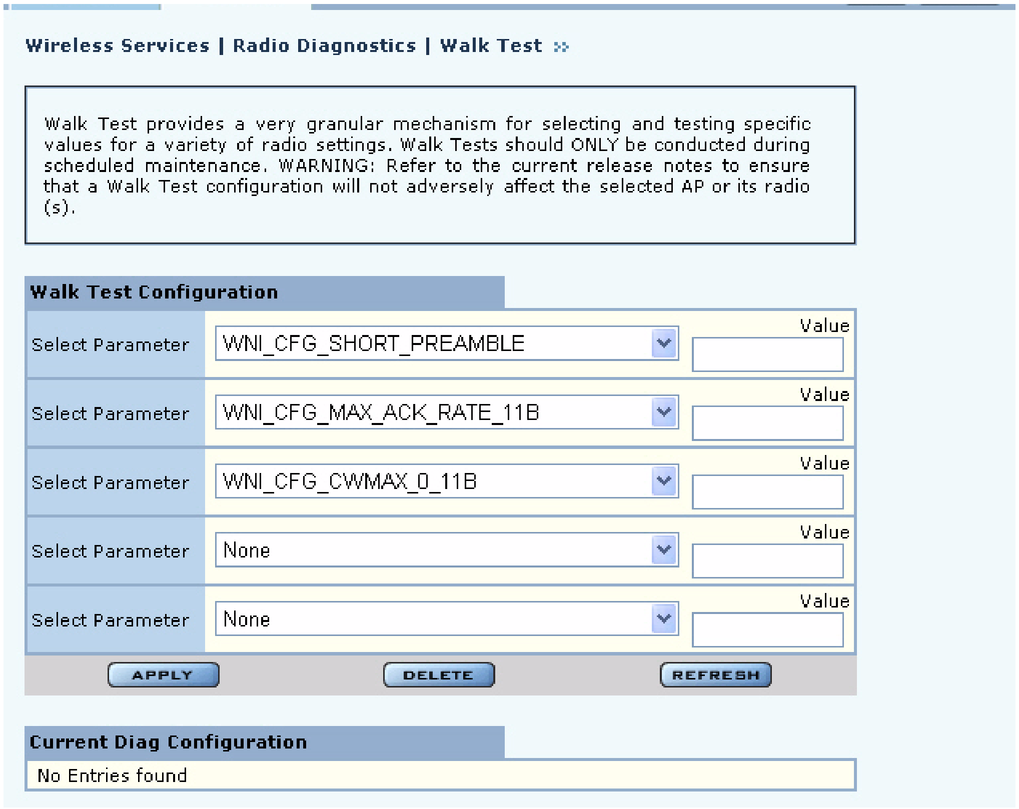
Click and drag to zoom. Double-click to unzoom.

Link Test Statistics [Uplink Signal Quality]

Walk Test

! **CAUTION:** These Radio Diagnostics are to be used only by Product Engineers. The information below is for reference only.

Figure 69: Radio Diagnostics - Walk Test



Wireless Services | Radio Diagnostics | Walk Test »

Walk Test provides a very granular mechanism for selecting and testing specific values for a variety of radio settings. Walk Tests should ONLY be conducted during scheduled maintenance. WARNING: Refer to the current release notes to ensure that a Walk Test configuration will not adversely affect the selected AP or its radio (s).

Walk Test Configuration

Select Parameter	WNI_CFG_SHORT_PREAMBLE	Value
Select Parameter	WNI_CFG_MAX_ACK_RATE_11B	Value
Select Parameter	WNI_CFG_CWMAX_0_11B	Value
Select Parameter	None	Value
Select Parameter	None	Value

Current Diag Configuration

No Entries found

Parameter	Parameter Description	Range/Units
WNI_CFG_CURRENT_TX_ANTENNA	#of TX chains	1 to 2 / +
WNI_CFG_CURRENT_RX_ANTENNA	# of RX chains	1 to 3 / –
WNI_CFG_DEFER_THRESHOLD	Packet Detection Threshold	0–254 / dBm + 130
WNI_CFG_ACK_TIMEOUT_11A	Ack Timeout 802.11a	0 - 100 / Micro seconds
WNI_CFG_ACK_TIMEOUT_11B	Ack Timeout 802.11b	0 - 100 / Micro seconds
WNI_CFG_MAX_ACK_RATE_11A	Max Ack Rate 802.11a	MAC rate encoding: Rate - Entered Value 6 - 12 9 - 18 12 - 24 18 - 36 24 - 48 36 - 72

Parameter (continued)	Parameter Description	Range/Units
WNI_CFG_MAX_ACK_RATE_11B	Max Ack Rate 802.11b	MAC rate encoding: Rate - Entered Value 1 - 2 2 - 4 5.5 - 11 11 - 22
WNI_CFG_SHORT_PREAMBLE	Enables or Disables Short Preamble	DISABLE (0), ENABLE (1)
WNI_CFG_CWMIN_0_11A	Min Contention Window Size for 802.11a (TC0)	0 - 1023 / slots
WNI_CFG_CWMIN_0_11B	Min Contention Window Size for 802.11b (TC0)	0 - 1023 / slots
WNI_CFG_CWMIN_0_11G	Min Contention Window Size for 802.11g (TC0)	0 - 1023 / slots
WNI_CFG_CWMAX_0_11A	Max Contention Window Size for 802.11a (TC0)	0 - 1023 / slots
WNI_CFG_CWMAX_0_11B	Max Contention Window Size for 802.11b (TC0)	0 - 1023 / slots
WNI_CFG_CWMAX_0_11G	Max Contention Window Size for 802.11g (TC0)	0 - 1023 / slots
WNI_CFG_PROXIMITY	Used to set the transmit power for radio	0 (operates at max power), 1 (operates at reduced power)

5 Configuring Networking Settings

This chapter explains how to configure the advanced networking features of the 108 Mbps Wireless Access Point. It includes the following topics:

- **Introduction**
- **Configuring Bridging Services**
- **Configuring IP Routes**
- **Configuring VLANs**
- **Configuring Quality of Service**
- **Configuring Advanced QoS**
- **Configuring Packet Filters**
- **Configuring Interfaces**
- **Configuring SNMP**
- **Ping Test**

Introduction

The 108 Mbps Wireless Access Point provides advanced features to configure wireless networking services and extend services to network users. From the Networking Services menu, assign interfaces, define quality of service, configure VLANs, and define packet filters. Statistics are also available to monitor network activity.

NOTE: It is not necessary to modify any of the default networking settings in order to get a wireless network up and running. The default settings may also be acceptable for normal operation of small to mid-size networks.

Interfaces

Figure 70 illustrates the physical and logical elements of an PLANEX wireless network. Each 108 Mbps Wireless Access Point has virtual interfaces that correspond to specific communications functions, as listed in Table 10. The interfaces wlan0 and wlan1 provide access to the BSS created on the AP radios; the interface eth0 provides access to the Ethernet network. In addition, a separate interface is reserved for each wireless backhaul trunk.

Figure 70: PLANEX Wireless Network Elements

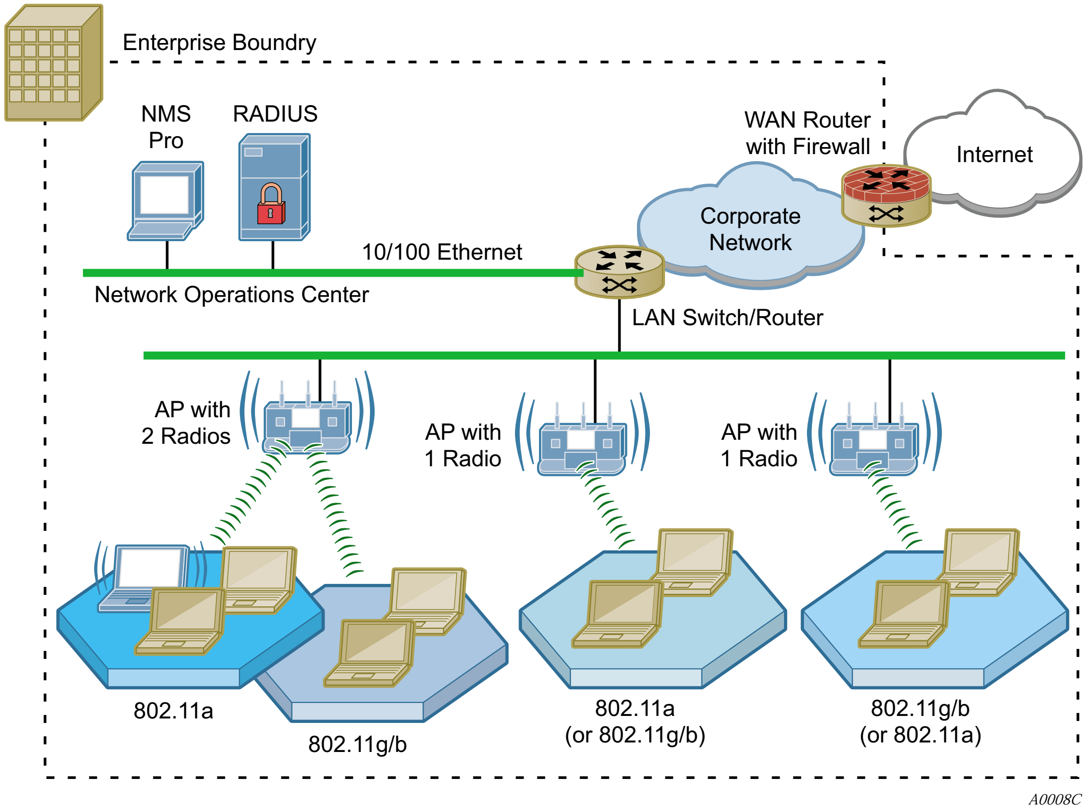


Table 10: AP Interfaces

Interface	Description
eth0	Wired Ethernet interface
wlan0	Wireless interface, radio 0
wlan1	Wireless interface, radio 1
wlan0.tkx	Backhaul x created on wlan0. Each radio can support multiple backhauls.
wlan1.tkx	Backhaul x created on wlan1. Each radio can support multiple backhauls.

Configuring Bridging Services

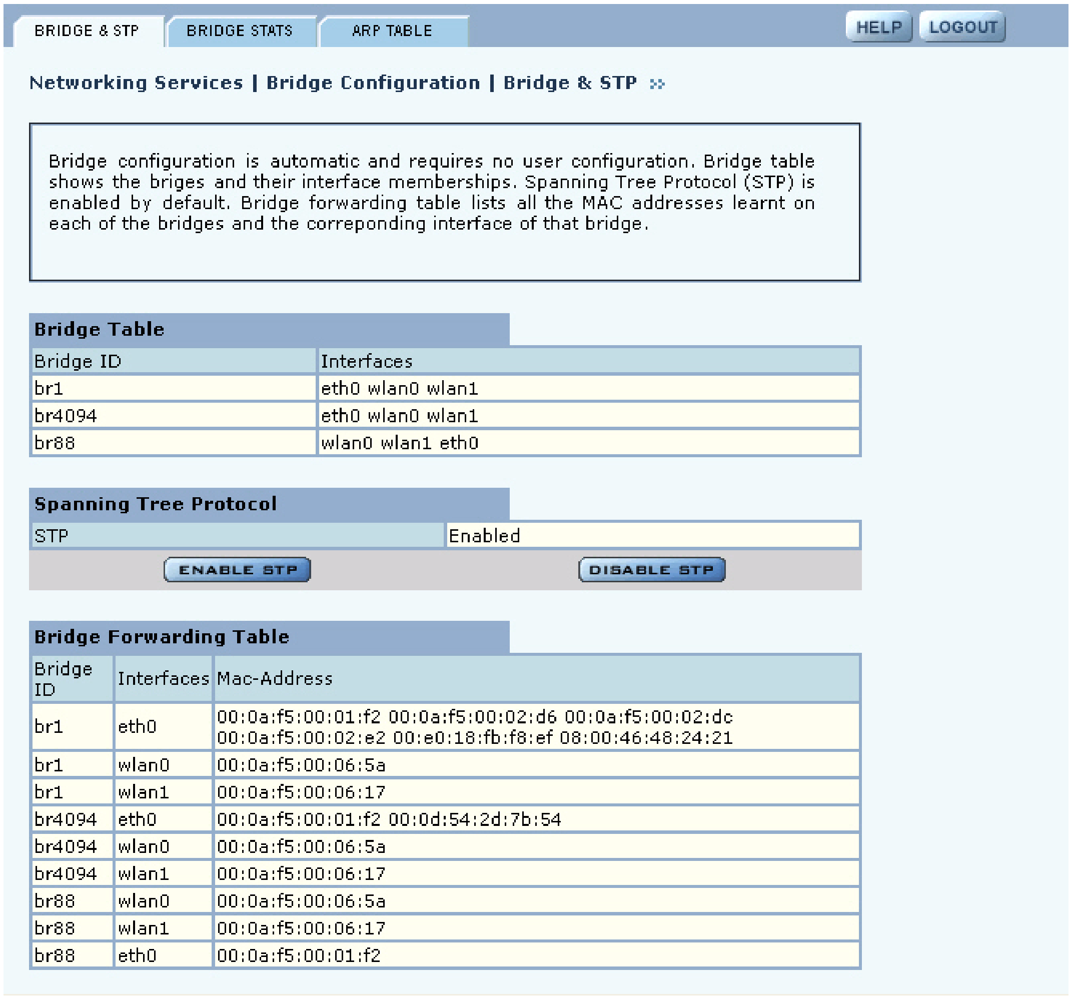
Use the Bridging panel, accessible from the Networking Services menu, to view the relationships among bridges, interfaces, and client stations. The panel contains the following tabs:

- Bridge & STP—View bridges, their interface members, and spanning tree protocol (STP) settings.
- Bridge Stats—View packet counts for each bridge.
- ARP Table—View the ARP cache.

Bridge and STP

Choose **Bridging** from the Networking Services menu to open the Bridge & STP tab (Figure 71), The tab displays how bridging is currently configured and lists the interfaces and MAC addresses learned at each interface (port) of the bridge. The bridge configuration is automatic and requires no user configuration.

Figure 71: Bridge Configuration - Bridge & STP



Networking Services | Bridge Configuration | Bridge & STP »

Bridge configuration is automatic and requires no user configuration. Bridge table shows the briges and their interface memberships. Spanning Tree Protocol (STP) is enabled by default. Bridge forwarding table lists all the MAC addresses learnt on each of the bridges and the correponding interface of that bridge.

Bridge Table

Bridge ID	Interfaces
br1	eth0 wlan0 wlan1
br4094	eth0 wlan0 wlan1
br88	wlan0 wlan1 eth0

Spanning Tree Protocol

STP	Enabled

Bridge Forwarding Table

Bridge ID	Interfaces	Mac-Address
br1	eth0	00:0a:f5:00:01:f2 00:0a:f5:00:02:d6 00:0a:f5:00:02:dc 00:0a:f5:00:02:e2 00:e0:18:fb:f8:ef 08:00:46:48:24:21
br1	wlan0	00:0a:f5:00:06:5a
br1	wlan1	00:0a:f5:00:06:17
br4094	eth0	00:0a:f5:00:01:f2 00:0d:54:2d:7b:54
br4094	wlan0	00:0a:f5:00:06:5a
br4094	wlan1	00:0a:f5:00:06:17
br88	wlan0	00:0a:f5:00:06:5a
br88	wlan1	00:0a:f5:00:06:17
br88	eth0	00:0a:f5:00:01:f2

Each bridge name is composed of a prefix, `br`, together with a bridge number. When the VLAN feature is enabled, the VLAN ID is used as the bridge number. `br1` represents VLAN 1 and is the default bridge for forwarding user data traffic. `br4094` represents VLAN 4094, which is an internal VLAN assigned to the default bridge used for the Spanning Tree Protocol (see “Spanning Tree Protocol (STP)” on page 103).

The Bridge table on the Summary tab lists each bridge and its associated interfaces (or ports). The Bridge Forwarding table, located at the bottom of the panel, lists each bridge and interface, and specifies which MAC addresses are learned at the interface.

Spanning Tree Protocol (STP)

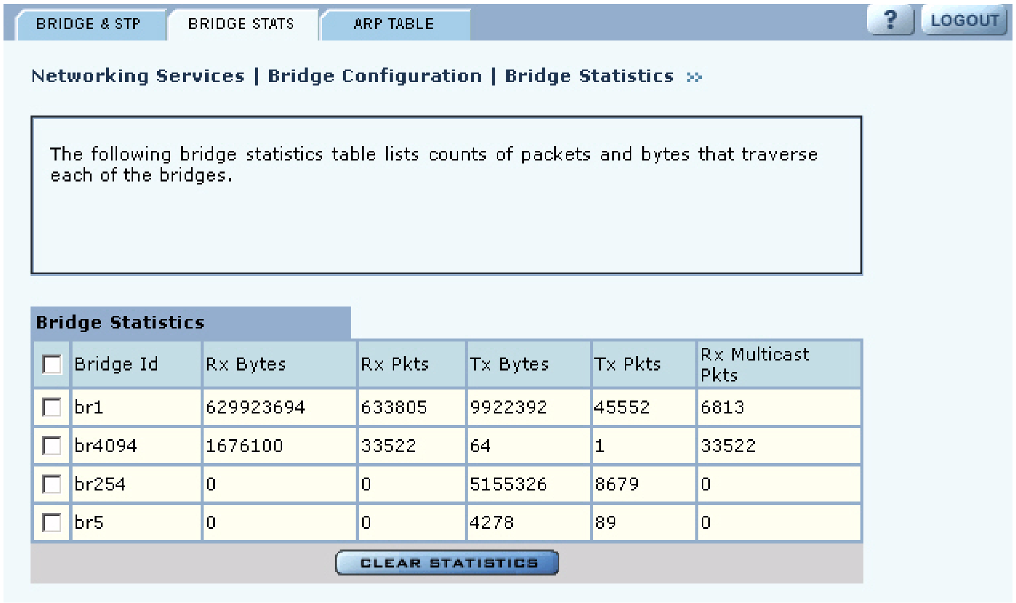
The Summary tab also provides an option for enabling or disabling Spanning Tree Protocol (STP). STP is a protocol that prevents bridging loops from forming due to incorrectly configured networks. STP provides protection against looping, but it does increase network overhead. Before STP allows traffic through a specific port, there may be a time lapse of 30 seconds. Operations may also take longer than normal.

The default setting for STP is `enabled`. Disable STP if the network is small to mid-size and looping is not a concern.

Bridge Statistics

The Bridge Stats tab (Figure 72) provides a summary of transmit/receive statistics for each bridge or VLAN. The statistics are calculated from the last time the AP was rebooted or the Clear Statistics button was selected. Click **Clear Statistics** to return the collected values to zero and start collecting statistics again.

Figure 72: Bridge Configuration - Bridge Stats



Networking Services | Bridge Configuration | Bridge Statistics »

The following bridge statistics table lists counts of packets and bytes that traverse each of the bridges.

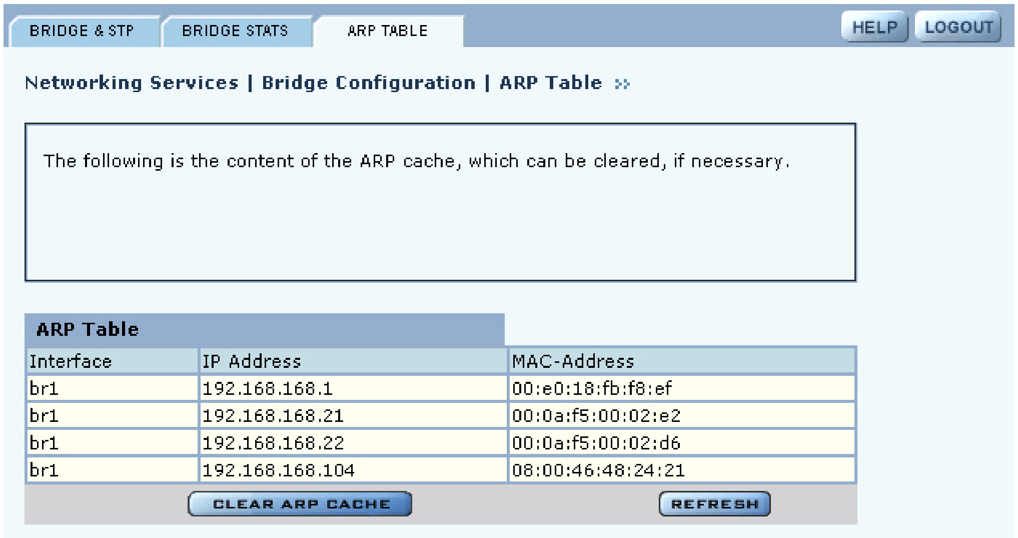
Bridge Statistics

□	Bridge Id	Rx Bytes	Rx Pkts	Tx Bytes	Tx Pkts	Rx Multicast Pkts
□	br1	629923694	633805	9922392	45552	6813
□	br4094	1676100	33522	64	1	33522
□	br254	0	0	5155326	8679	0
□	br5	0	0	4278	89	0

ARP Table

The Address Resolution Protocol (ARP) tab (Figure 73) displays the current mapping of IP addresses to MAC addresses associated with the listed interface. During normal operations, the ARP table is updated automatically based on the number of MAC entities in the network. If a mapping changes, however, some entries of the ARP table may become invalid. In this case, click **Clear ARP Cache** on the tab to remove the current ARP entries and repopulate the table automatically with valid entries. Click **Refresh** to update the display.

Figure 73: Bridge Configuration - ARP Table



Networking Services | Bridge Configuration | ARP Table

The following is the content of the ARP cache, which can be cleared, if necessary.

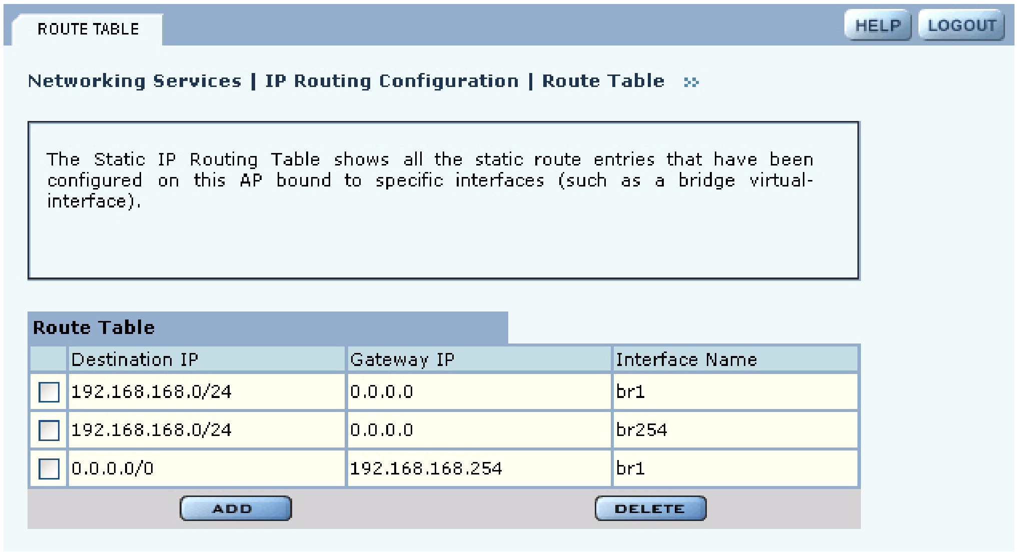
ARP Table

Interface	IP Address	MAC-Address
br1	192.168.168.1	00:e0:18:fb:f8:ef
br1	192.168.168.21	00:0a:f5:00:02:e2
br1	192.168.168.22	00:0a:f5:00:02:d6
br1	192.168.168.104	08:00:46:48:24:21

Configuring IP Routes

IP routing expands the addressing capability of the 108 Mbps Wireless AP and allows you to mange the AP from outside its local subnet. Use the IP Routing panel (Figure 73) to explicitly address subnets that are not local. If a destination subnet is not entered into this panel, then default network routing applies.

Figure 74: IP Routing



Networking Services | IP Routing Configuration | Route Table

The Static IP Routing Table shows all the static route entries that have been configured on this AP bound to specific interfaces (such as a bridge virtual-interface).

Route Table

	Destination IP	Gateway IP	Interface Name
□	192.168.168.0/24	0.0.0.0	br1
□	192.168.168.0/24	0.0.0.0	br254
□	0.0.0.0/0	192.168.168.254	br1

The Route table shows the static route entries currently configured on the AP and bound to bridging interfaces. To create a new route, click **Add**, enter the following information, and click **Save**.

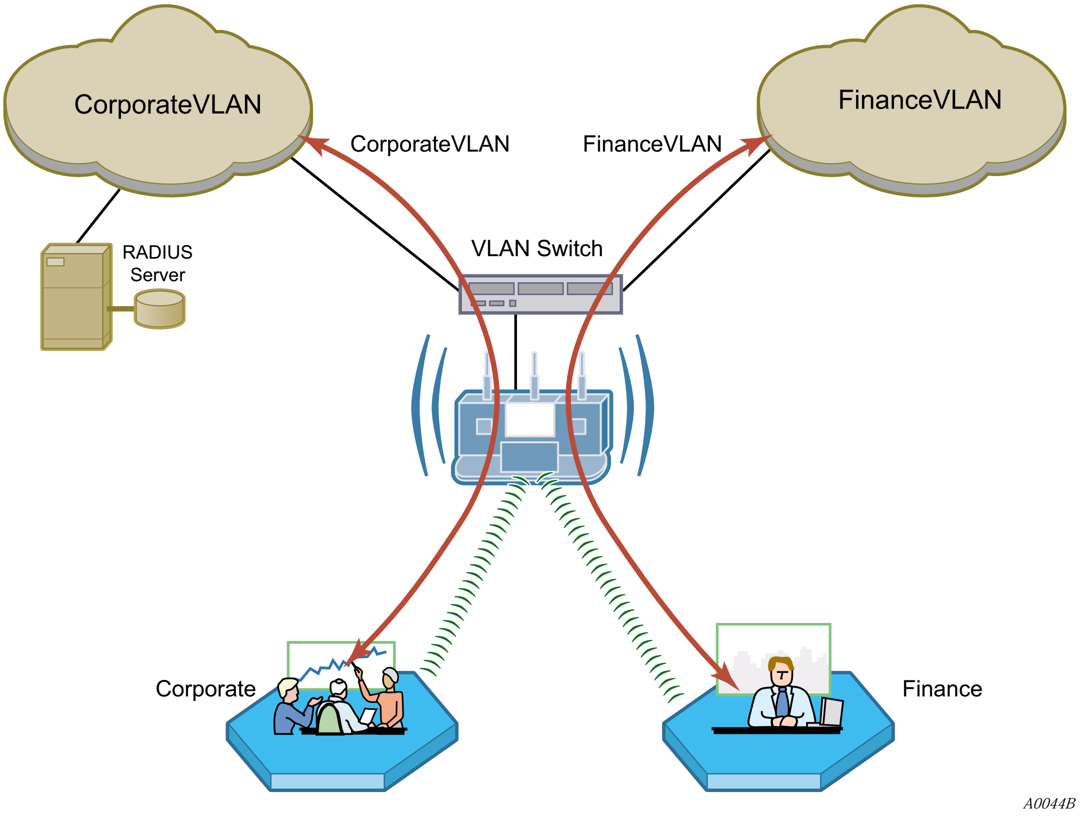
Field	Description
Destination IP	Enter the IP address of the subnet to which packets can be forwarded, along with the subnet prefix for the address.

Field	Description
Gateway IP	Enter the IP address of the gateway that will route traffic between this AP and the destination subnet.
Interface Name	Enter the name of the bridging interface. Use the `br` prefix, as described in "Configuring Bridging Services" on page 102.

Configuring VLANs

VLANs are key to helping enterprises improve network traffic flow, increase load, and deliver varying levels of service and access to different groups of users. For example, Figure 75 shows how Acme Works uses two VLANs: one for normal corporate traffic and one for Finance Department traffic. When a Finance Department user logs in to the network, the Finance group tag is passed to the 108 Mbps Wireless AP, and the Finance service profile, including Finance VLAN, is applied to the user. Database transaction traffic, which was previously a burden on the overall network, is now handled through the Finance VLAN and is transparent to normal corporate users.

Figure 75: Example Use of VLANs to Manage Enterprise Traffic



The 108 Mbps Wireless AP supports up to 16 VLANs including the default VLAN. Use the VLAN Configuration panel, accessible from the Networking Services menu, to add new VLANs and map VLANs to specific AP interfaces. The VLAN panel contains a list of users assigned to user VLANs; to make user VLAN assignments, use service profiles ("SSIDs and Service Profiles" on page 80).

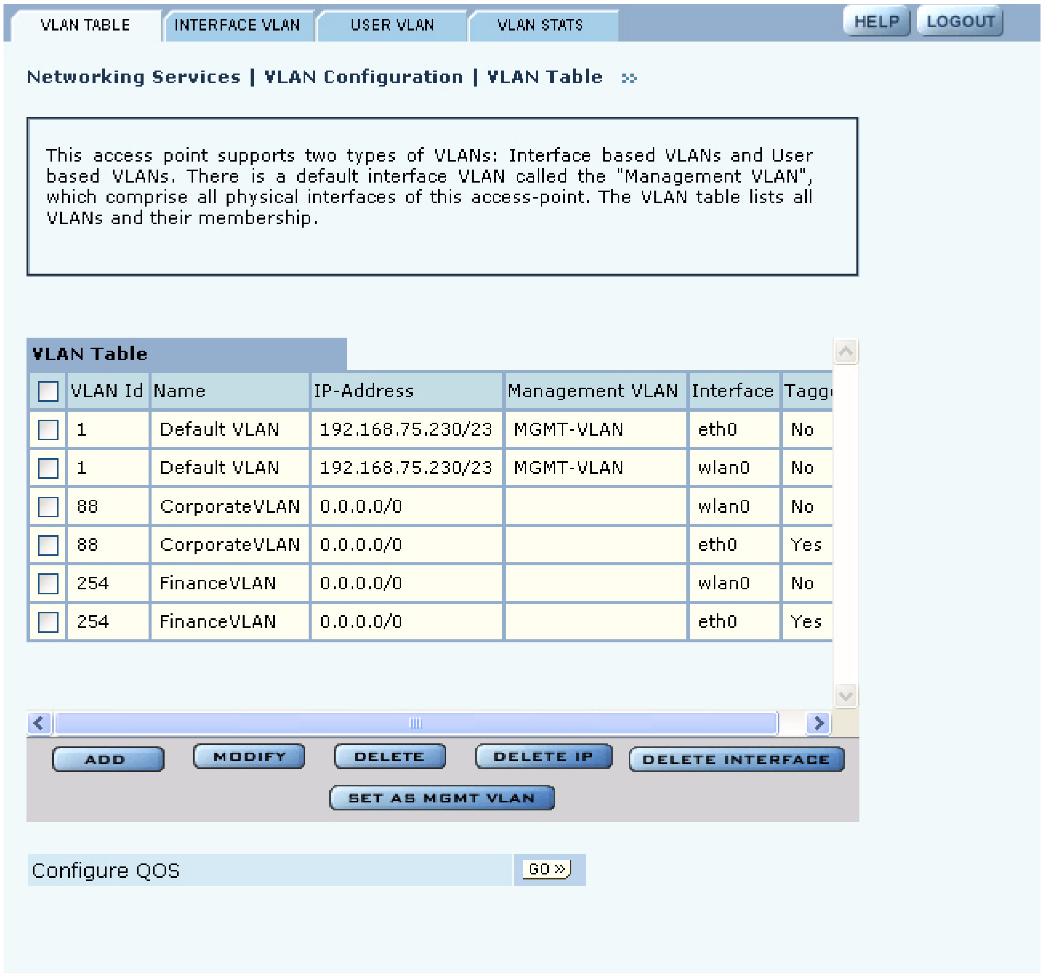
The VLAN Configuration panel contains the following tabs:

- VLAN Table—View the list of currently defined VLANs and add or modify VLANs.
- Interface VLAN—Assign VLANs for untagged frames arriving at the AP.
- User VLAN—View the list of users assigned to each VLAN by virtue of user group membership.
- VLAN Stats—View packet statistics for each VLAN.

VLAN Table

Choose **VLAN** from the Networking Services menu to list information about each VLAN and interface (Figure 76).

Figure 76: VLAN Configuration - VLAN Table



Networking Services | VLAN Configuration | VLAN Table »

This access point supports two types of VLANs: Interface based VLANs and User based VLANs. There is a default interface VLAN called the "Management VLAN", which comprise all physical interfaces of this access-point. The VLAN table lists all VLANs and their membership.

VLAN Table

□	VLAN Id	Name	IP-Address	Management VLAN	Interface	Tagg
□	1	Default VLAN	192.168.75.230/23	MGMT-VLAN	eth0	No
□	1	Default VLAN	192.168.75.230/23	MGMT-VLAN	wlan0	No
□	88	CorporateVLAN	0.0.0.0/0		wlan0	No
□	88	CorporateVLAN	0.0.0.0/0		eth0	Yes
□	254	FinanceVLAN	0.0.0.0/0		wlan0	No
□	254	FinanceVLAN	0.0.0.0/0		eth0	Yes

Configure QOS

The VLAN table contains the following columns of information:

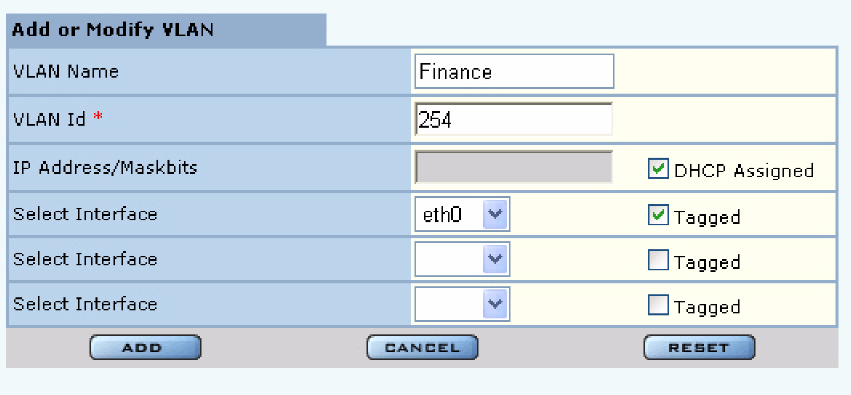
Field	Description
VLAN ID	Identifier for the VLAN. In bridging notation, this is the numeric ID that follows the `br` prefix.
Name	Alphanumeric name of the VLAN. The field is optional, unless it is the default VLAN. The maximum length of VLAN Name is 80 characters.
IP Address	The IP address and subnet prefix assigned to the VLAN. Assigning an IP address enables the VLAN to be managed from this AP.
Management VLAN	Indication of whether this VLAN is the management VLAN or not.
Interface	The logical AP interface. The table contains a separate row for each VLAN/ interface combination.

Field	Description
Tagged	Indication of whether the identity of the VLAN is explicitly encoded in transmitted packets. Each frame contains a four-byte tag that encodes the VLAN to which the packet belongs when it is sent on a tagged interface. If the received packet is untagged, the packet is classified as belonging to the interface VLAN. If the VLAN interface is not tagged, then the AP drops any VLAN-tagged packet. When the packet is transmitted from the interface, it is be untagged.

Use the buttons on the Summary tab to add a new VLAN, configure an existing VLAN, delete an interface from a VLAN, delete IP addresses from a VLAN, or set an interface as part of the management VLAN. The default VLAN cannot be modified.

To add a new VLAN, click **Add** to open the Add VLAN Entry panel (Figure 77).

Figure 77: VLAN Configuration - Add VLAN Entry Panel



Add or Modify VLAN

VLAN Name	Finance	
VLAN Id *	254	
IP Address/Maskbits		☑ DHCP Assigned
Select Interface	eth0	☑ Tagged
Select Interface		□ Tagged
Select Interface		□ Tagged

Enter the following information to define the new VLAN:

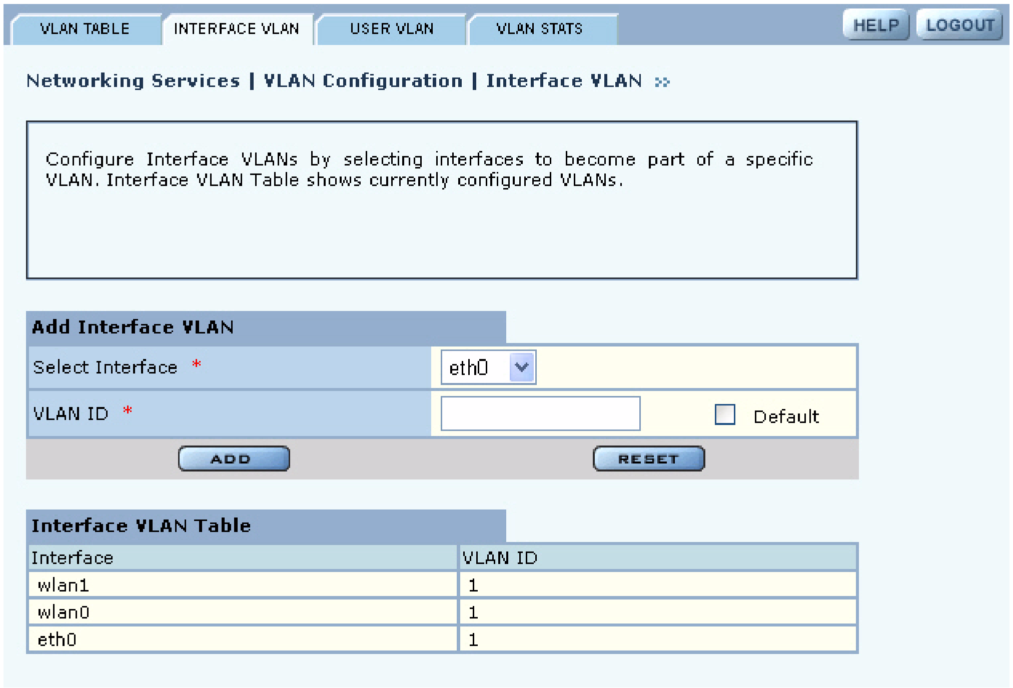
Field	Description
VLAN Name	Enter an alphanumeric name for the VLAN. The maximum length of VLAN name is 80 characters. (optional)
VLAN ID	Enter a numeric identifier for the VLAN. This number is used for table references and as part of the bridging ID. The range is 2 - 4093. (required)
IP Address/Maskbits	Enter the IP address and maskbits used to access the VLAN for management purposes. If the address is to be assigned by a DHCP server, select **DHCP Assigned**. If the VLAN is to be used for guest access, you must assign an IP address. See “Configuring Guest Access” on page 158
Select Interface	Select interfaces for the VLAN. If an interface is assigned to the VLAN, then packets transmitted over that interface are included in that VLAN.
Tagged	Select **Tagged** for an interface to mark packets sent out over the interface as belonging to the VLAN.

Click **Apply** to create the new VLAN and return to the VLAN table.

Interface VLAN

When the AP receives a frame, it must determine the VLAN to which the frame belongs. If the received frame is tagged, then VLAN is already known, and the AP can route the packet accordingly. The Interface VLAN tab (Figure 78) specifies treatment of frames that arrive at the AP in an untagged state. Each interface is assigned to a VLAN, which then receives all untagged frames arriving at the interface.

Figure 78: VLAN Configuration - Interface VLAN



Networking Services | VLAN Configuration | Interface VLAN

Configure Interface VLANs by selecting interfaces to become part of a specific VLAN. Interface VLAN Table shows currently configured VLANs.

Add Interface VLAN

Select Interface *	eth0
VLAN ID *	□ Default

Interface VLAN Table

Interface	VLAN ID
wlan1	1
wlan0	1
eth0	1

Make sure that the VLAN is defined before assigning an interface, and then configure the following fields:

Field	**Description**
Select Interface	Select the AP interface.
VLAN ID	Enter the VLAN ID. (required)
Default	Select to assign this as the default VLAN for untagged frames.

Click **Add** to assign the interface to the specified VLAN.

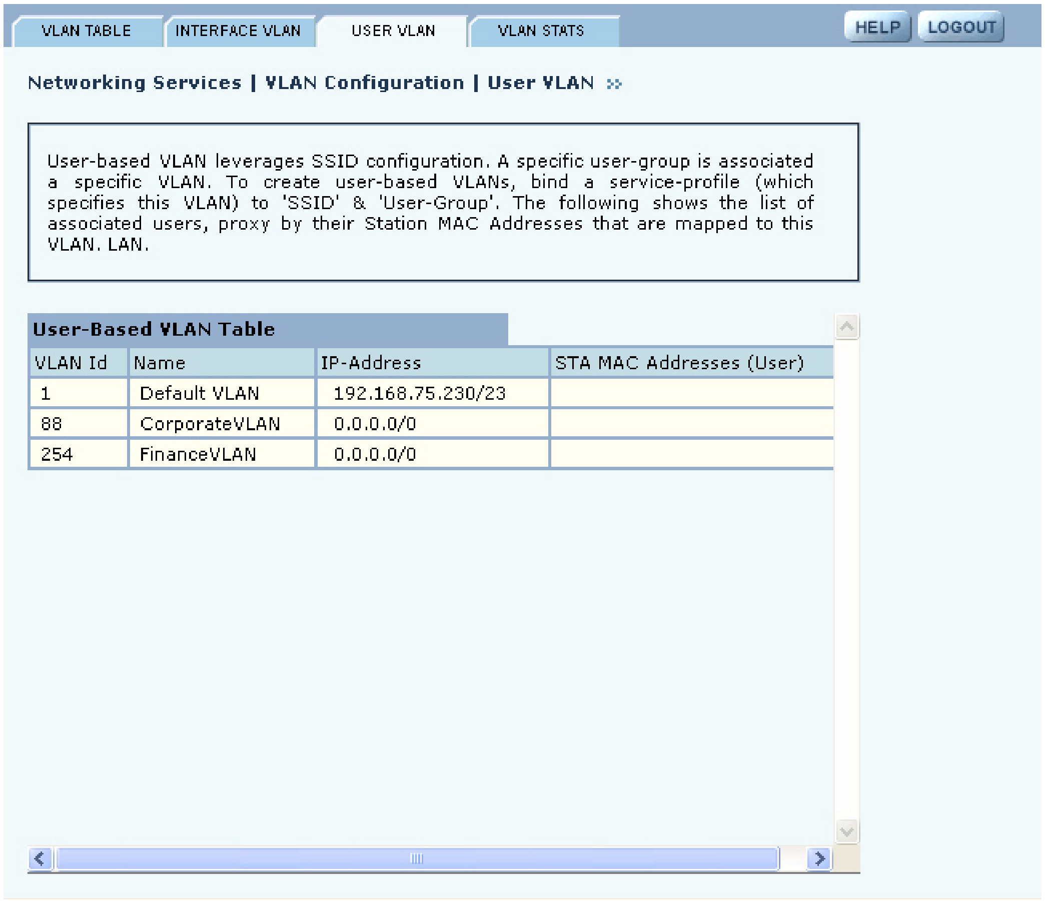
User VLAN

The read-only User VLAN tab (Figure 79) lists the client stations mapped to each VLAN by way of bound service profiles. The tab contains the following information:

Field	**Description**
VLAN ID	VLAN identifier
VLAN name	Alphanumeric name of the VLAN
IP Address	Address used to access the VLAN
MAC Address	MAC addresses of the client stations that are mapped to this VLAN through their user group’s service profile

See “Configuring SSID Parameters” on page 79 for information on service profiles.

Figure 79: VLAN - User VLAN



Networking Services | VLAN Configuration | User VLAN

User-based VLAN leverages SSID configuration. A specific user-group is associated a specific VLAN. To create user-based VLANs, bind a service-profile (which specifies this VLAN) to 'SSID' & 'User-Group'. The following shows the list of associated users, proxy by their Station MAC Addresses that are mapped to this VLAN. LAN.

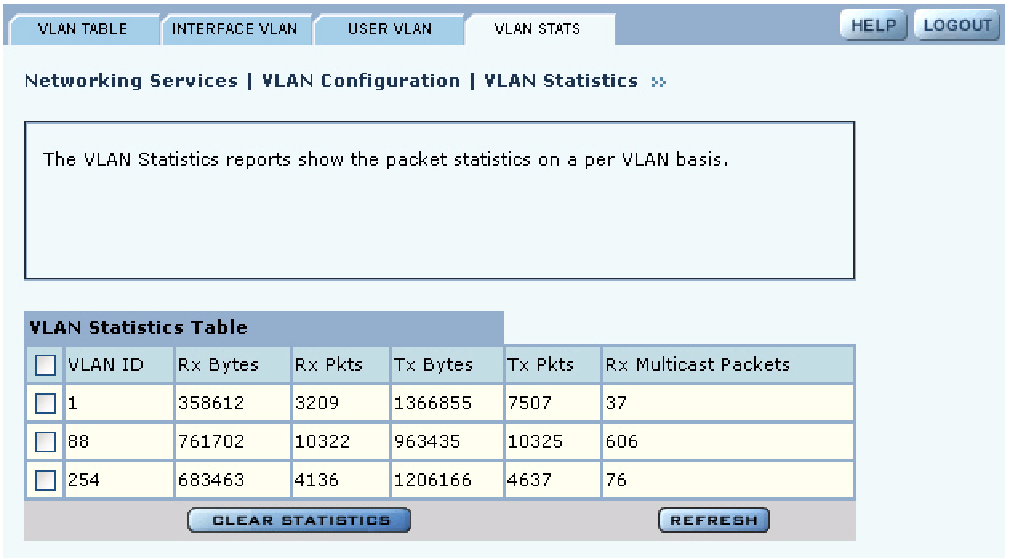
User-Based VLAN Table

VLAN Id	Name	IP-Address	STA MAC Addresses (User)
1	Default VLAN	192.168.75.230/23	
88	CorporateVLAN	0.0.0.0/0	
254	FinanceVLAN	0.0.0.0/0	

VLAN Statistics

The VLAN Stats tab (Figure 80) provides a summary of transmit/receive statistics for each VLAN. The statistics are calculated from the last time that the AP was rebooted or the Clear Statistics button was selected. Click **Refresh** to update the statistics or **Clear Statistics** to return the collected values to zero and start collecting statistics again.

Figure 80: VLAN - Stats



The VLAN Statistics reports show the packet statistics on a per VLAN basis.

VLAN Statistics Table

□	VLAN ID	Rx Bytes	Rx Pkts	Tx Bytes	Tx Pkts	Rx Multicast Packets
□	1	358612	3209	1366855	7507	37
□	88	761702	10322	963435	10325	606
□	254	683463	4136	1206166	4637	76

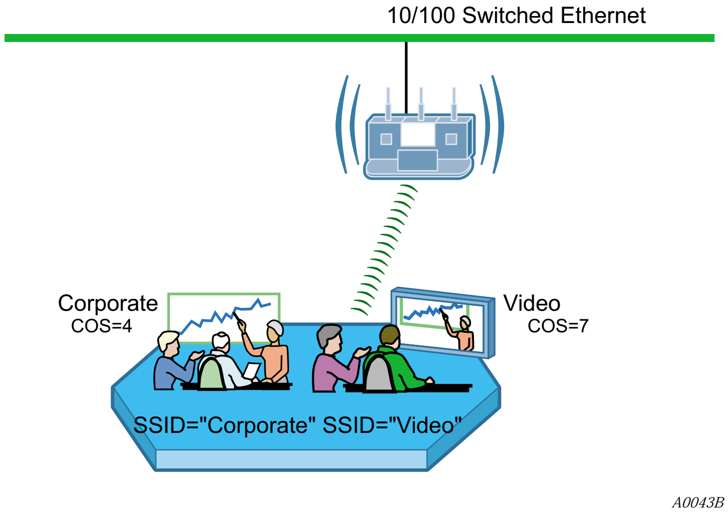
Configuring Quality of Service

Under normal network conditions, traffic in the wireless network is routed on a best-effort basis, and all types of traffic are treated with equal priority. Quality of Service (QoS) permits priority setting for different types of traffic, which can be important for applications in which even minor interruptions in packet transmission can have a deleterious effect on perceived results. Examples include streaming media or voice-over-IP (VoIP). With a QoS process in place, multiple clients can run applications with varying traffic delivery requirements over a single shared network.

PLANEX supports QoS through hierarchical classes of service (COS) that control how network bandwidth is shared among multiple entities. COS specifies a numeric class code with values ranging from 0 (lowest priority) to 7 (highest priority). This method does not guarantee bandwidth for different traffic types, but does assure that high COS traffic will be given preference.

For example, when Acme Works wanted to set up a video conference center, it was important to provide a higher quality of service for the video conference application. The company accordingly set up a structure of multiple SSIDs in which a higher COS value was assigned to the service profile for the Video SSID (Figure 81).

Figure 81: Example Applications with Different COS Levels



The 108 Mbps Wireless AP supports several options for assigning COS to the packets passing into the AP (the *ingress* to the AP).

Rule	Description
TCID-to-COS mapping	Defines a COS mapping based on the Traffic Class Identifier (TCID), which is part of the standard 802.11 frame header. Incoming packets with a TCID value assigned can be mapped to COS.
VLAN-to-COS	Defines a COS mapping for packets that are not VLAN-tagged upon arrival at the AP.
Interface-to-COS	Associates a COS value to each of the AP interfaces (eth0, wlan0, wlan1).
MAC	Uses the COS value from the user group’s service profile (see “Configuring SSID Parameters” on page 79).

Rule (continued)	Description
IP Precedence	Defines a mapping based on the first 3 bits in the Type of Service (TOS) byte of the IP header. Incoming packets that have an IP Precedence value can be mapped to COS.
DiffServ Code point (DSCP)-to-COS	Defines a mapping based on the first 6 bits in the TOS byte of the IP header. Incoming packets that have a DSCP value can be mapped to COS.
IP Protocol	Assigns COS value based on the standard numbers for individual IP protocols.
Class Order	Determines the order in which all the COS mapping rules are applied.

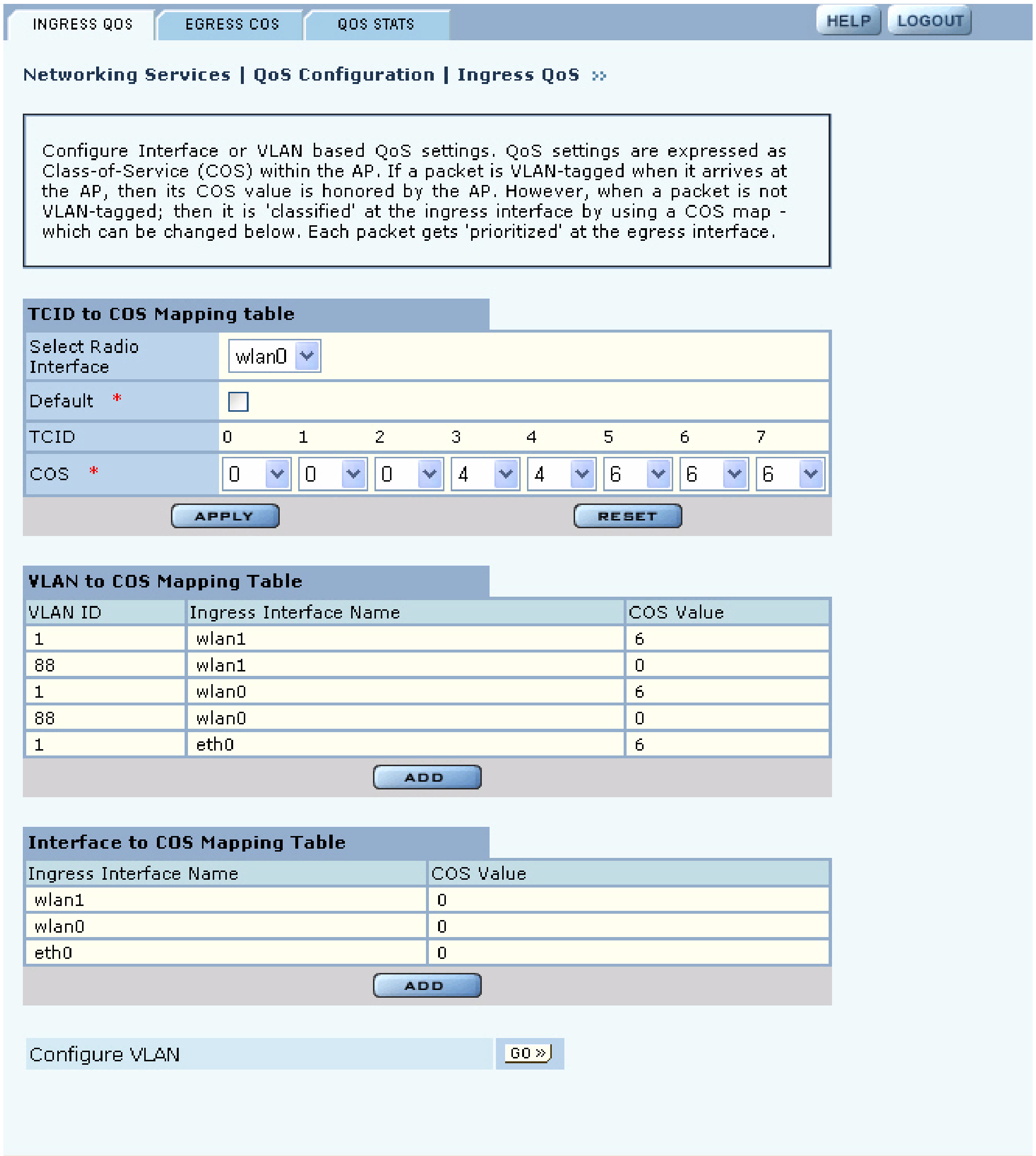
Use the QoS Configuration panel to define TCID, VLAN, and Interface COS mappings. Use the Advanced QoS Configuration panel (“Configuring Advanced QoS” on page 117) to define the IP and DSCP mapping and to assign class order.The QoS Configuration panel is divided into the following tabs:

- Ingress QOS—Define COS mappings packets entering the AP.
- Egress COS—Assign priority to the 802.11 packets leaving the AP.
- QOS Stats—Display QoS statistics for each of the AP interfaces.

Ingress QOS

Use the Ingress QOS tab to assign COS values to incoming 802.11 packets. If a packet has a COS value in the VLAN tag when it arrives at the AP, then its COS value is honored by the AP. If the packet is not VLAN-tagged, then it can be classified at the ingress interface by way of a COS map defined on the Ingress QOS tab (Figure 82).

Figure 82: QOS Configuration - Ingress QOS



Networking Services | QoS Configuration | Ingress QoS »

Configure Interface or VLAN based QoS settings. QoS settings are expressed as Class-of-Service (COS) within the AP. If a packet is VLAN-tagged when it arrives at the AP, then its COS value is honored by the AP. However, when a packet is not VLAN-tagged; then it is 'classified' at the ingress interface by using a COS map - which can be changed below. Each packet gets 'prioritized' at the egress interface.

TCID to COS Mapping table

Select Radio Interface	wlan0							
Default *	□							
TCID	0	1	2	3	4	5	6	7
COS *	0	0	0	4	4	6	6	6

VLAN to COS Mapping Table

VLAN ID	Ingress Interface Name	COS Value
1	wlan1	6
88	wlan1	0
1	wlan0	6
88	wlan0	0
1	eth0	6

Interface to COS Mapping Table

Ingress Interface Name	COS Value
wlan1	0
wlan0	0
eth0	0

Perform the following functions on this tab:

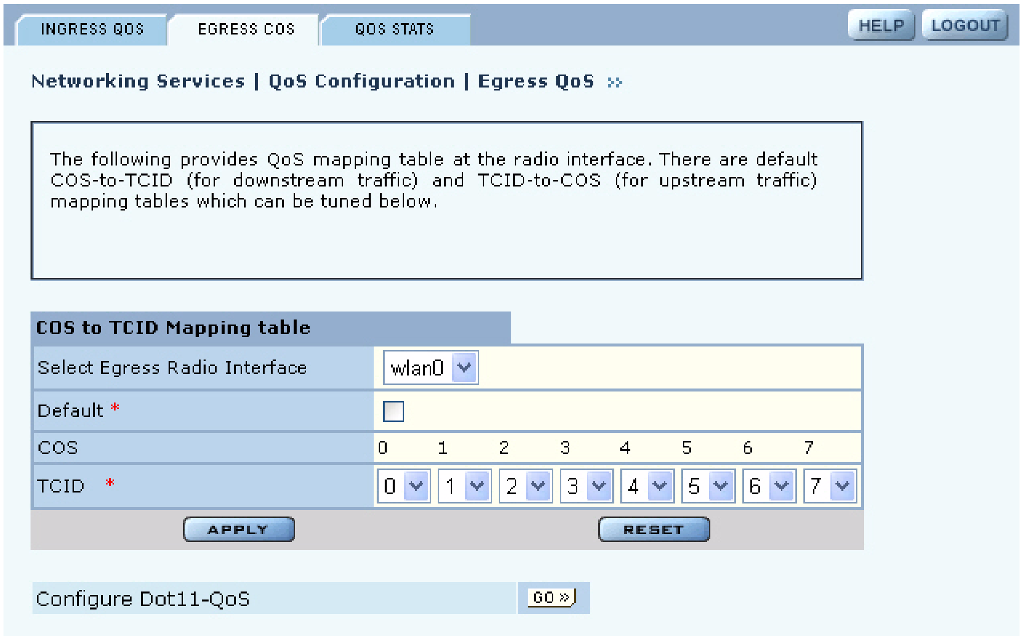
Function	Steps
Define TCID to COS mapping	**1** Select the radio interface for the mapping. **2** Select a COS value for each TCID value, or select **Default** to accept the default mapping. **3** Click **Apply**.
Define VLAN-to-COS mapping	**1** Click **Add**. **2** Select the AP interface. **3** Select the VLAN ID. (See “Configuring VLANs” on page 107 for information on VLAN IDs.) **4** Select a COS value or select **Default** to use the default mapping. **5** Click **Apply**.
Interface-to-COS	**1** Click **Add**. **2** Select the AP interface. **3** Select a COS value or select **Default** to use the default mapping. **4** Click **Apply**.

Egress COS

Use the Egress COS tab (Figure 84) to modify the default priorities assigned to 802.11 packets leaving the AP by creating a COS-to-TCID mapping.

If a TCID to COS mapping is defined, the TCID value is obtained from the mapping table of the interface based on the COS field of the frame. By default, COS-to-TCID mapping is one-to-one, i.e. COS 0 maps TCID 0, 1 maps to 1, … and 7 maps to 7. If your network supports fewer than 8 priority levels, you can map multiple COS levels to a single TCID value.

Figure 83: **QOS Configuration - Egress COS**



Networking Services | QoS Configuration | Egress QoS »

The following provides QoS mapping table at the radio interface. There are default COS-to-TCID (for downstream traffic) and TCID-to-COS (for upstream traffic) mapping tables which can be tuned below.

COS to TCID Mapping table

Select Egress Radio Interface	wlan0							
Default *	□							
COS	0	1	2	3	4	5	6	7
TCID *	0	1	2	3	4	5	6	7

Configure Dot11-QoS

Configure the following fields on this tab:

Field	Description
Select Radio Interface	Select the AP interface.
Default	Select to use the default mapping.
TCID	If Default is not selected, map each COS level to a TCID level.

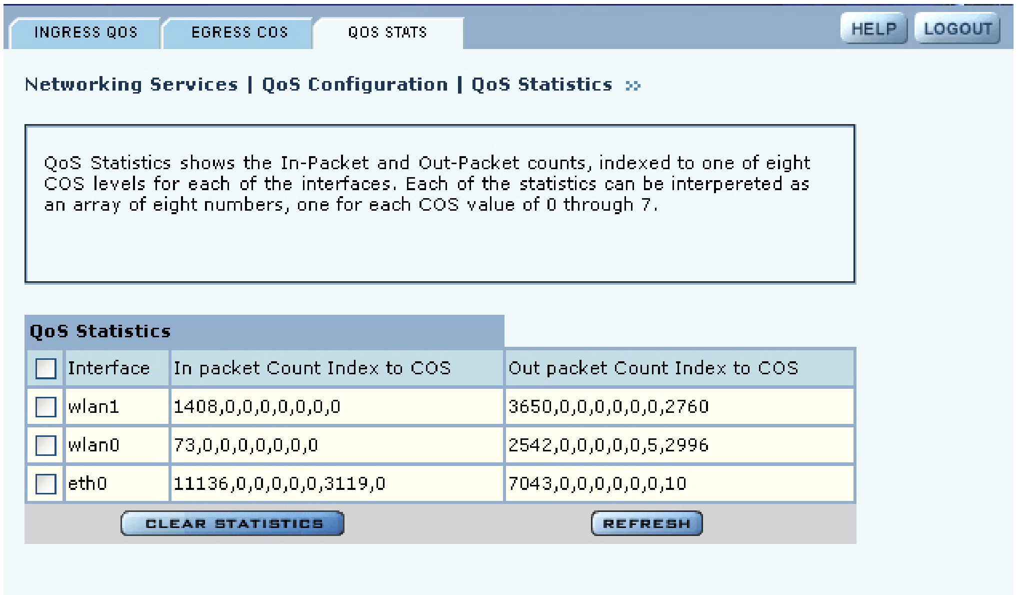
Click **Apply** to save your changes or **Reset** to return to previously saved values.

QoS Stats

The QoS Stats tab (Figure 84) presents incoming packet and outgoing packet counts for each of the AP interfaces. The counts are indexed to one of the eight available COS levels. Every statistic is a comma-separated set of numbers, each of which corresponds to one of the COS levels: 0-7. For example, the out-of-packet count for wlan0 in the figure shows 77614 packets at COS level 0 and 36127 packets at COS level 7.

Click **Clear Statistics** to return the values to zero and restart the collection process.

Figure 84: QOS Configuration - QOS Stats



Networking Services | QoS Configuration | QoS Statistics »

QoS Statistics shows the In-Packet and Out-Packet counts, indexed to one of eight COS levels for each of the interfaces. Each of the statistics can be interpereted as an array of eight numbers, one for each COS value of 0 through 7.

QoS Statistics

□	Interface	In packet Count Index to COS	Out packet Count Index to COS
□	wlan1	1408,0,0,0,0,0,0,0	3650,0,0,0,0,0,0,2760
□	wlan0	73,0,0,0,0,0,0,0	2542,0,0,0,0,0,5,2996
□	eth0	11136,0,0,0,0,0,3119,0	7043,0,0,0,0,0,0,10

Configuring Advanced QoS

Use the Advanced QoS panel to assign COS values to packets entering the AP based on IP layer information and choose the QoS class order. The panel contains the following tabs:

- Class-Order—Determine the order in which to apply all the QoS rules.
- IP-DSCP—Define COS mapping based on the first 6 bits in the TOS byte of the IP header.
- IP Protocol—Use standard IP protocol numbers assigned to different IP layer protocols.
- IP Precedence—Define COS mapping based on the first 3 bits in the TOS byte of the IP header.

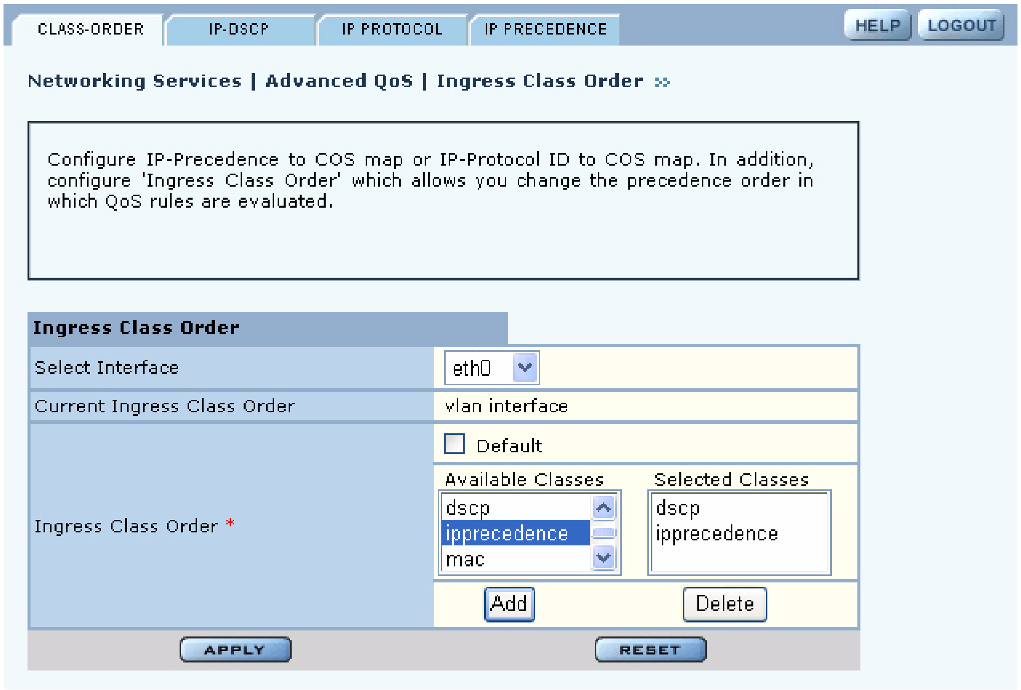
Class-Order

The COS mappings on the QoS and Advanced QoS Configuration panels may yield conflicting results for ingress packet priority. Use the Class-Order tab (Figure 84) to specify the order in which to apply each of the rules. When a packet arrives at the AP, the AP checks to see whether a mapping exists for the first rule in the class-order list. If so, that mapping is applied to the packet. If not, the AP checks whether a mapping exists for the second rule. If so, that mapping is applied. If not, the AP continues down the class-order list.

The default class order is:

- TCID
- IP Protocol
- DSCP
- IP Precedence
- MAC
- VLAN
- Interface

Figure 85: Advanced QOS Configuration - Class-Order



Networking Services | Advanced QoS | Ingress Class Order »

Configure IP-Precedence to COS map or IP-Protocol ID to COS map. In addition, configure 'Ingress Class Order' which allows you change the precedence order in which QoS rules are evaluated.

Ingress Class Order	
Select Interface	eth0
Current Ingress Class Order	vlan interface
Ingress Class Order *	□ Default Available Classes: dscp, ipprecedence, mac Selected Classes: dscp, ipprecedence

Configure the following fields on the Class-Order tab:

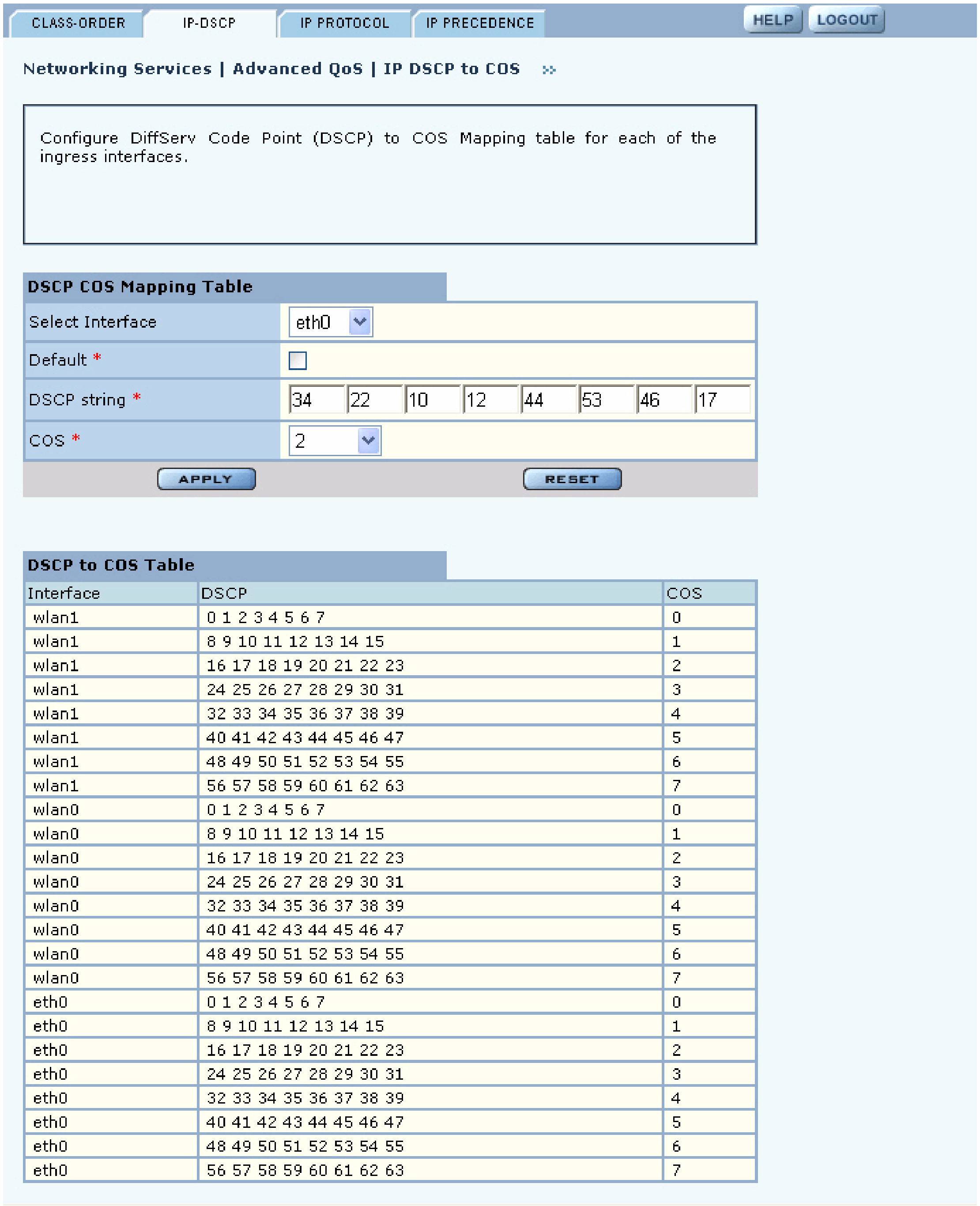
Field	Description
Select Radio Interface	Select the AP interface.
Ingress Class Order - Default	Select to use the default mapping.
Ingress Class Order - Move to Top	If the default order is not chosen, select a COS mapping type and click **Apply** to move it to the top of the class-order priority list. Repeat as needed to create the desired ordering.

Click **Apply** to save all the changes on the tab.

IP-DSCP

Use the IP-DSCP tab (Figure 86) to map DiffServ Code point (DSCP) values to COS and to view the current DSCP to COS maps. DSCP uses the first 6 bits in the TOS byte of the IP header, so the possible values range from 0 to 63.

Figure 86: Advanced QOS Configuration - IP-DSCP



Networking Services | Advanced QoS | IP DSCP to COS »

Configure DiffServ Code Point (DSCP) to COS Mapping table for each of the ingress interfaces.

DSCP COS Mapping Table

Select Interface	eth0
Default *	□
DSCP string *	34 22 10 12 44 53 46 17
COS *	2

DSCP to COS Table

Interface	DSCP	COS
wlan1	0 1 2 3 4 5 6 7	0
wlan1	8 9 10 11 12 13 14 15	1
wlan1	16 17 18 19 20 21 22 23	2
wlan1	24 25 26 27 28 29 30 31	3
wlan1	32 33 34 35 36 37 38 39	4
wlan1	40 41 42 43 44 45 46 47	5
wlan1	48 49 50 51 52 53 54 55	6
wlan1	56 57 58 59 60 61 62 63	7
wlan0	0 1 2 3 4 5 6 7	0
wlan0	8 9 10 11 12 13 14 15	1
wlan0	16 17 18 19 20 21 22 23	2
wlan0	24 25 26 27 28 29 30 31	3
wlan0	32 33 34 35 36 37 38 39	4
wlan0	40 41 42 43 44 45 46 47	5
wlan0	48 49 50 51 52 53 54 55	6
wlan0	56 57 58 59 60 61 62 63	7
eth0	0 1 2 3 4 5 6 7	0
eth0	8 9 10 11 12 13 14 15	1
eth0	16 17 18 19 20 21 22 23	2
eth0	24 25 26 27 28 29 30 31	3
eth0	32 33 34 35 36 37 38 39	4
eth0	40 41 42 43 44 45 46 47	5
eth0	48 49 50 51 52 53 54 55	6
eth0	56 57 58 59 60 61 62 63	7

Configure the following fields on this tab:

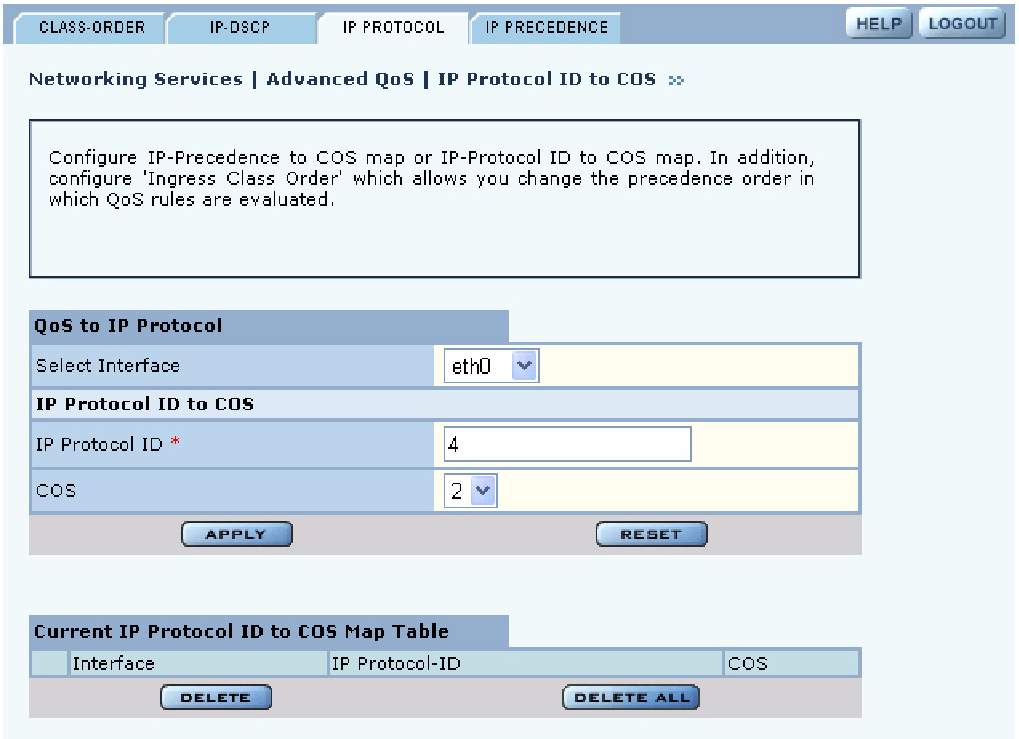
Field	Description
Select Radio Interface	Select the AP interface.
Default	Select to use the default mapping.
DSCP String	If Default is not chosen, enter up to eight DSCP values that you want to map to a specific COS value.
COS	Select the COS value.

Click **Apply** to save all the changes on the tab.

IP Protocol

Use the IP Protocol tab (Figure 87) to base the COS mapping on IP protocol numbers, as defined in Version 4 of the IP protocol. Current protocol number assignments are available at http://www.iana.org.

Figure 87: Advanced QOS Configuration - IP Protocol



Networking Services | Advanced QoS | IP Protocol ID to COS

Configure IP-Precedence to COS map or IP-Protocol ID to COS map. In addition, configure 'Ingress Class Order' which allows you change the precedence order in which QoS rules are evaluated.

QoS to IP Protocol

Select Interface	eth0
IP Protocol ID to COS	
IP Protocol ID *	4
COS	2

Current IP Protocol ID to COS Map Table

	Interface	IP Protocol-ID	COS

Configure the following fields to define the IP Protocol-to-COS map:

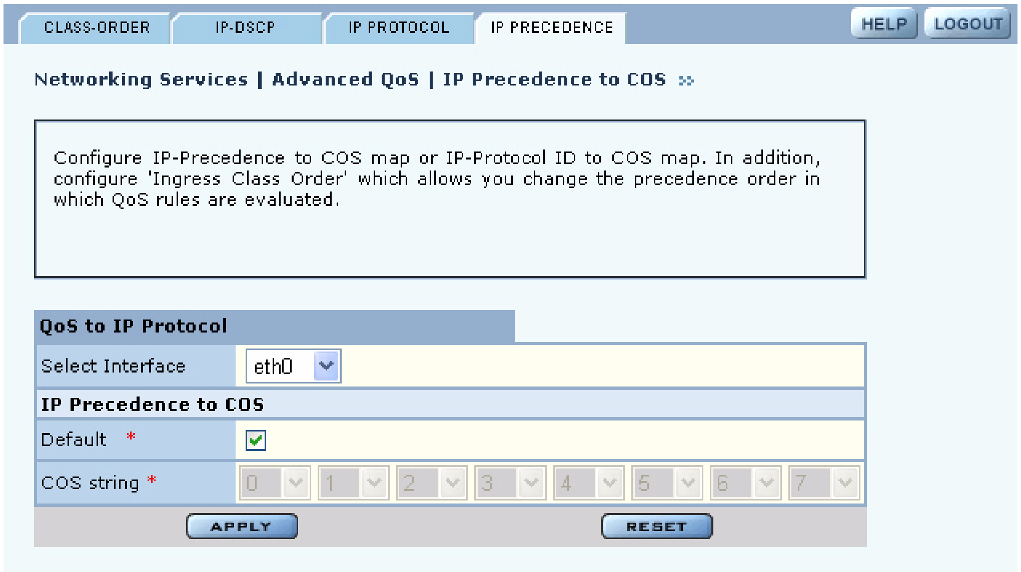
Field	Description
Select Radio Interface	Select the AP interface.
IP Protocol ID	Enter the number assigned to the IP protocol.
COS	Select the COS value.

Click **Apply** to save all the changes on the tab.

IP Precedence

Use the IP Precedence tab (Figure 88) to base the COS mapping on the first 3 bits in the TOS byte of the IP header.

Figure 88: Advanced QOS Configuration - IP Precedence



Networking Services | Advanced QoS | IP Precedence to COS »

Configure IP-Precedence to COS map or IP-Protocol ID to COS map. In addition, configure 'Ingress Class Order' which allows you change the precedence order in which QoS rules are evaluated.

QoS to IP Protocol

Select Interface	eth0
IP Precedence to COS	
Default *	☑
COS string *	0 1 2 3 4 5 6 7

Configure the following fields to define an IP Precedence-to-COS map:

Field	Description
Select Radio Interface	Select the AP interface.
Default	Select to apply the default mapping
COS	If Default is not chosen, select the desired COS values.

Click **Apply** to save all the changes on the tab.

Configuring Packet Filters

Use the Filter Configuration panel, accessible from the Networking Services menu, to define packet filtering rules for the specific AP interfaces. Filters can help improve performance by reducing load on the wireless side of the network.

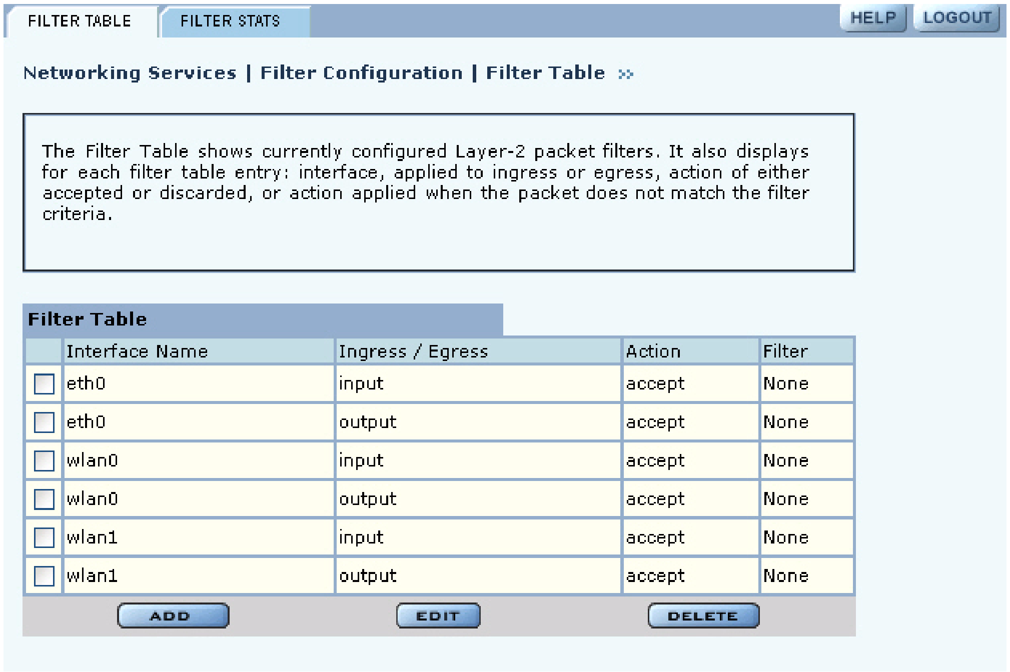
The panel contains the following tabs:

- Filter Table—View currently-defined packet filters and add or edit filters.
- Filter Stats—View counts of packets that match the filter criteria.

Filter Table

Choose **Filter Configuration** from the Networking Services menu to open the Filter Table tab (Figure 89). By default, an incoming and outgoing filter is defined for each of the interfaces wlan0, wlan1, and eth0. The Filter table displays the name of the interface, whether it is for incoming or outgoing traffic, whether to accept or discard the packet, and the criterion used to accept or discard it.

Figure 89: Filter Configuration - Filter Table



The Filter Table shows currently configured Layer-2 packet filters. It also displays for each filter table entry: interface, applied to ingress or egress, action of either accepted or discarded, or action applied when the packet does not match the filter criteria.

Filter Table

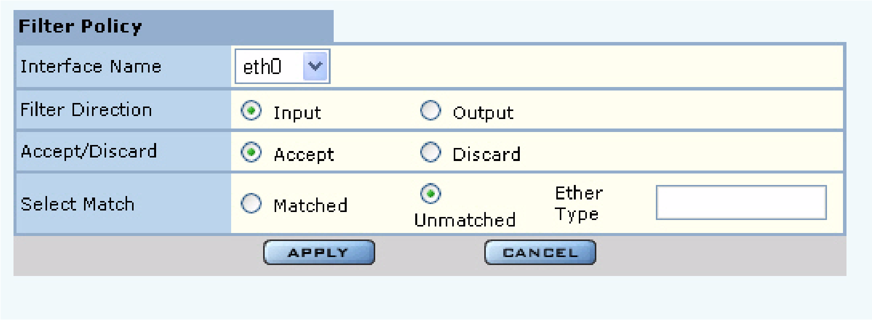
	Interface Name	Ingress / Egress	Action	Filter
□	eth0	input	accept	None
□	eth0	output	accept	None
□	wlan0	input	accept	None
□	wlan0	output	accept	None
□	wlan1	input	accept	None
□	wlan1	output	accept	None

From the Filter Table tab, add a new filter by clicking **Add**, or edit an existing one by selecting the filter and clicking **Edit**. The Add Filter Entry panel opens(Figure 90). Enter or select values for the following fields:

Field	Description
Interface Name	If creating a new filter, select an interface from the pull-down list.
Filter Direction	Specify whether the filter is for incoming (ingress) or outgoing (egress) communications. It is necessary to create a separate filter for each.
Accept/Discard	Indicate whether the filtering rule is to accept or discard the packet.
Select Match	Indicate if the filter rule is satisfied when a packet contains an Ether Type value that matches the specified Ether Type, or if the filter rule is satisfied when a packet contains an Ether Type that does not match any other filter rule. Ether Type is the standard Ethernet code for the type of packet (e.g., for IP, the code is 2048, or 0x800 hex).

Click **Apply** to save the values and return to the Summary tab. Click **Cancel** to return to the Summary tab without saving the values.

Figure 90: Filter Configuration - Add Filter Entry Panel



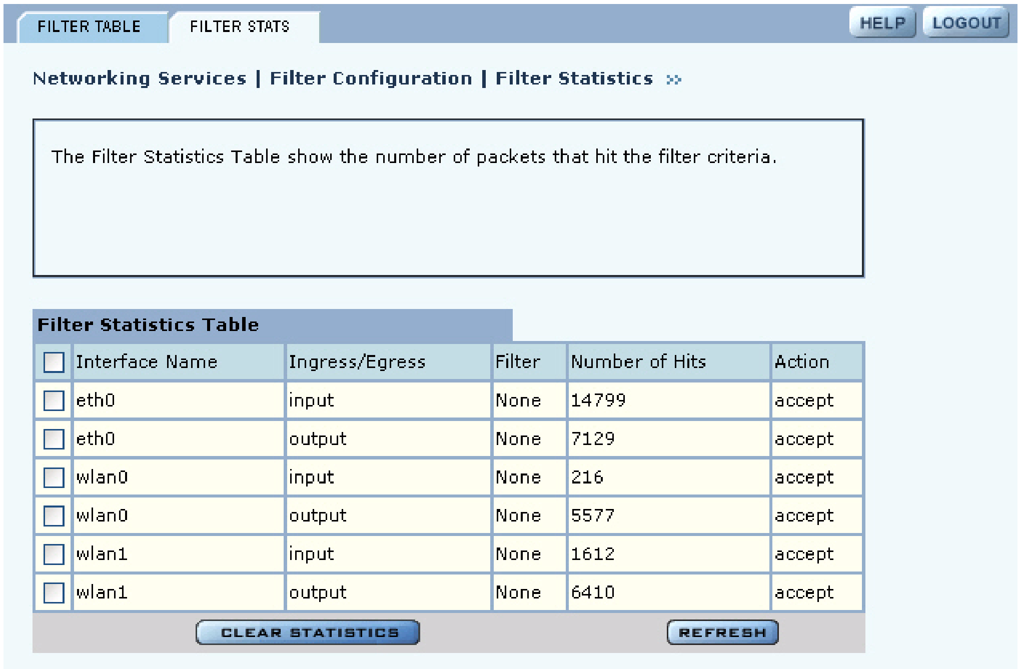
Filter Policy

Interface Name	eth0			
Filter Direction	● Input	○ Output		
Accept/Discard	● Accept	○ Discard		
Select Match	○ Matched	● Unmatched	Ether Type	

Filter Statistics

The Filter Stats tab (Figure 91) lists statistics for each defined filter. The statistics are calculated from the last time that the AP was rebooted or the Clear Statistics button was selected. The Hits column shows the number of packets of the specified type received on the interface with the defined filter. Click **Refresh** to update the statistics or **Clear Statistics** to return the collected values to zero and start collecting statistics again.

Figure 91: Filter Configuration - Stats Tab



Networking Services | Filter Configuration | Filter Statistics >>

The Filter Statistics Table show the number of packets that hit the filter criteria.

Filter Statistics Table

□	Interface Name	Ingress/Egress	Filter	Number of Hits	Action
□	eth0	input	None	14799	accept
□	eth0	output	None	7129	accept
□	wlan0	input	None	216	accept
□	wlan0	output	None	5577	accept
□	wlan1	input	None	1612	accept
□	wlan1	output	None	6410	accept

Configuring Interfaces

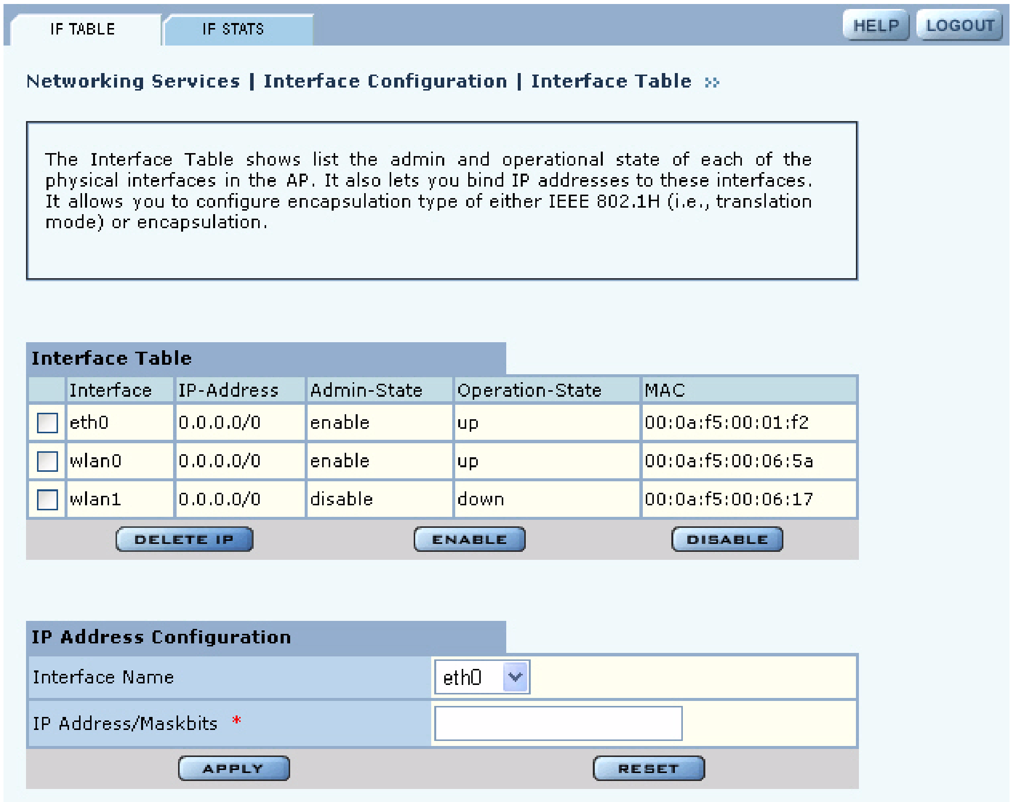
Use the Interface Configuration panel, accessible from the Networking Services menu, to configure the physical AP interfaces (wlan0, wlan1, eth0). The panel contains the following tabs:

- IF Table—View the administrative and operation state of each of the interfaces, and bind an IP address to each interface.
- IF Stats—View the packet and byte statistics for traffic traversing each interface.

Interface Table

Choose **Interface** from the Networking Services menu to open the Interface Table (Figure 92). Use this tab to assign an IP address to each interface, thereby making it possible to route traffic to the interface. Without an assigned IP address, traffic can only be bridged to the interface, not routed.

Figure 92: Interface Configuration - IF Table



Networking Services | Interface Configuration | Interface Table

The Interface Table shows list the admin and operational state of each of the physical interfaces in the AP. It also lets you bind IP addresses to these interfaces. It allows you to configure encapsulation type of either IEEE 802.1H (i.e., translation mode) or encapsulation.

Interface Table

	Interface	IP-Address	Admin-State	Operation-State	MAC
□	eth0	0.0.0.0/0	enable	up	00:0a:f5:00:01:f2
□	wlan0	0.0.0.0/0	enable	up	00:0a:f5:00:06:5a
□	wlan1	0.0.0.0/0	disable	down	00:0a:f5:00:06:17

IP Address Configuration

Interface Name	eth0
IP Address/Maskbits *	

The Interface table lists each interface along with its IP address, enabled or disabled flag, and indication of whether the interface is currently operational. Enable, disable, or delete an IP address assigned to an interface by selecting the interface entry and clicking **Enable**, **Disable**, or **Delete-IP**.

To assign an IP address to an interface, enter the following values under IP Address Configuration, and click **Apply**:

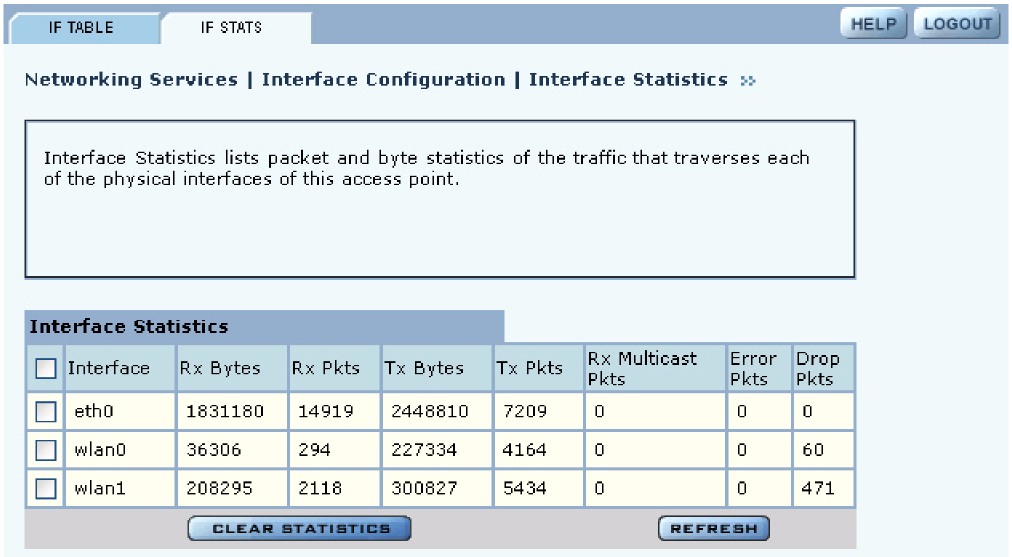
Field	Description
Interface Name	Select the AP interface name from the pull-down list
IP Address	Enter the IP address to assign to the interface (required)
Maskbits	Enter the subnet prefix length for the IP address (required)

Use the Encapsulation Configuration section at the bottom of the tab to ensure that the AP can operate with older equipment that is not fully 802.11-compatible. 802.1h is the current standard for encapsulation. For other, incompatible equipment, select **Encapsulated** to encase the Ethernet frames from the equipment within standard 802.11 frames. Click **Apply** after making any change.

Interface Statistics

The Interface Statistics tab (Figure 93) shows packet and byte statistics for each of the AP interfaces. The statistics are calculated from the last time that the AP was rebooted or the Clear Statistics button was selected. Click **Refresh** to update the statistics or **Clear Statistics** to return the collected values to zero and start collecting statistics again.

Figure 93: Interface - Stats Tab



Networking Services | Interface Configuration | Interface Statistics »

Interface Statistics lists packet and byte statistics of the traffic that traverses each of the physical interfaces of this access point.

Interface Statistics

□	Interface	Rx Bytes	Rx Pkts	Tx Bytes	Tx Pkts	Rx Multicast Pkts	Error Pkts	Drop Pkts
□	eth0	1831180	14919	2448810	7209	0	0	0
□	wlan0	36306	294	227334	4164	0	0	60
□	wlan1	208295	2118	300827	5434	0	0	471

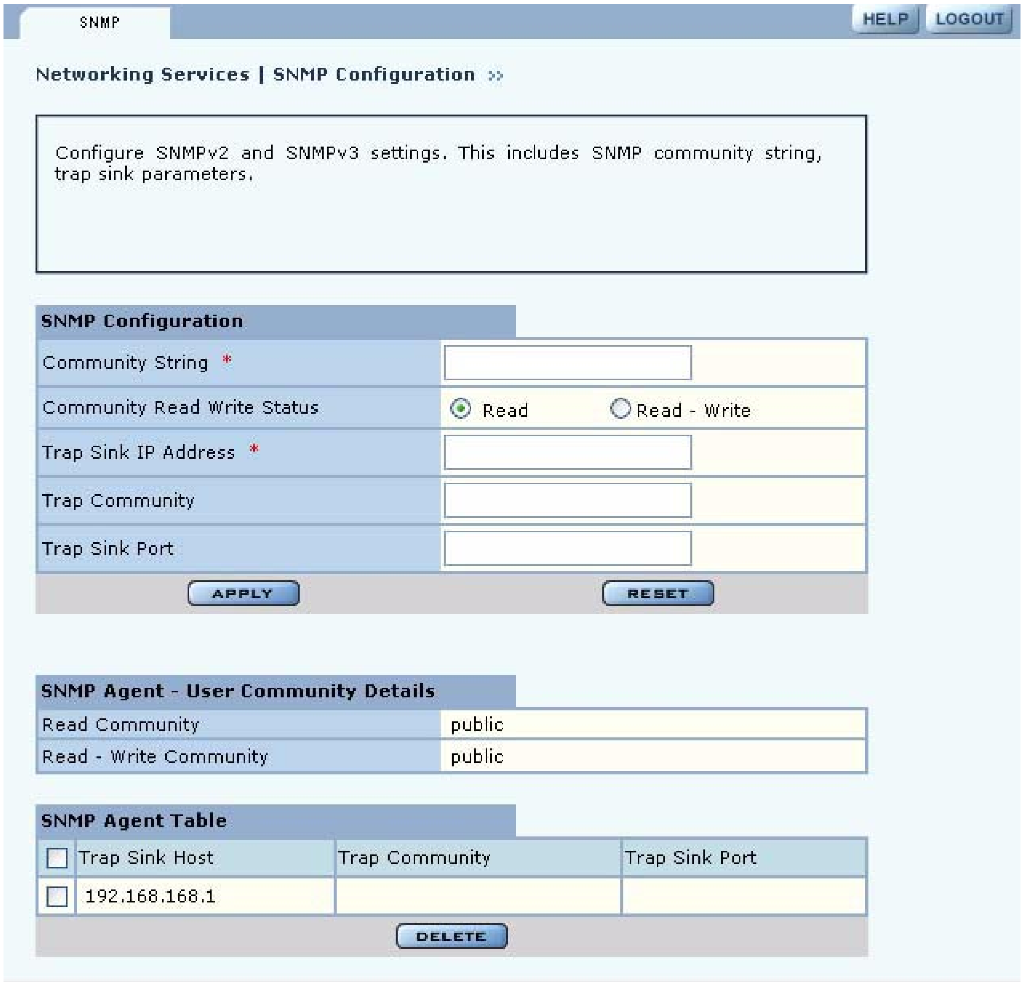
Configuring SNMP

Simple Network Management Protocol (SNMP) is an industry standard protocol used to manage interactions with the 108 Mbps Wireless APs. The protocol works through message passing between SNMP managers and agents, which are devices that comply with the SNMP protocol. The information of interest to the SNMP manager is stored in the agents' management information bases (MIBs) and sent to the SNMP manager upon request.

SNMP communities restrict access to the MIBs to authorized agents. Each community can be earmarked with read or read/write status, indicating the type of authorized MIBs access. An SNMP trap filters the SNMP messages and saves or drops them, depending upon how the system is configured.

Choose **SNMP Configuration** from the Networking Services menu to open the SNMP panel (Figure 94) to configure SNMP parameters.

Figure 94: SNMP Configuration



Networking Services | SNMP Configuration »

Configure SNMPv2 and SNMPv3 settings. This includes SNMP community string, trap sink parameters.

SNMP Configuration

Community String *	
Community Read Write Status	● Read ○ Read - Write
Trap Sink IP Address *	
Trap Community	
Trap Sink Port	

APPLY RESET

SNMP Agent - User Community Details

Read Community	public
Read - Write Community	public

SNMP Agent Table

□	Trap Sink Host	Trap Community	Trap Sink Port
□	192.168.168.1		

DELETE

Enter values in the following fields to define the basic SNMP configuration:

Field	Description
Community String	Enter the alphanumeric community string (required)
Community Read/Write Status	Indicate the read or read/write status of the community
Trap Sink IP Address	Enter the IP address where SNMP traps should be sent (required)
Trap Community	Enter the community for SNMP traps
Trap Sink Port	Indicate the port identified for the SNMP traps (default is 162)

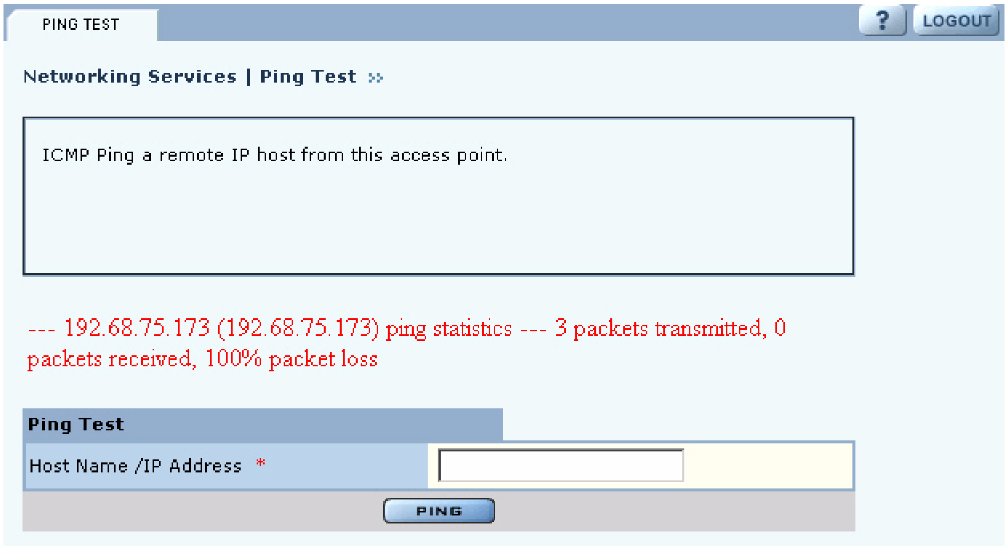
Click **Apply** to save your changes, or **Reset** to return to previously saved values.

The bottom of the SNMP panel contains a table of currently defined traps. To delete a trap, select it in the SNMP Agent Table, and click **Delete**.

Ping Test

Use the Ping Test panel to execute an ICMP Echo Request to check network connectivity to a remote IP host. Enter the hostname or IP address of the remote host. Figure 95 shows the Ping Test panel with test results presented.

Figure 95: Ping Test



ICMP Ping a remote IP host from this access point.

--- 192.68.75.173 (192.68.75.173) ping statistics --- 3 packets transmitted, 0 packets received, 100% packet loss

Ping Test	
Host Name /IP Address *	

6 Configuring a Wireless Backhaul

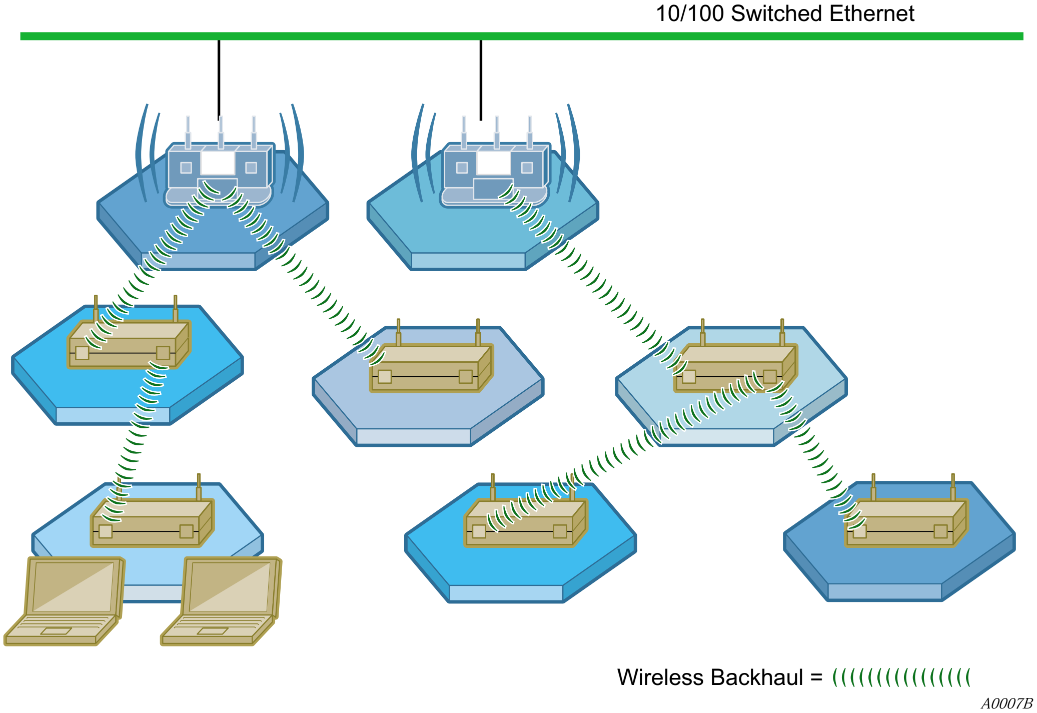
This chapter explains how to set up a wireless distribution system to cover a large area with limited wired network connectivity. It covers the following topics:

- **Introduction**
- **Setting Up a Wireless Backhaul**

Introduction

Wireless backhaul refers to the process of delivering data from a node on the wireless network back to the wired network. In a wireless backhaul configuration, some APs connect directly to the wired network, while others relay wireless signals from clients to the APs that are connected to the wired network. Wireless backhaul interconnects multiple 108 Mbps Wireless Access Points to form a wireless distribution system, in which an 802.11x network covers large areas, such as a campus or open area with relatively few wired access points (Figure 96).

Figure 96: Wireless Backhaul Network



Applications of wireless backhaul include building-to-building bridging and 802.11b traffic aggregation. PLANEX support for wireless backhaul includes bridge creation, instantiation of logical bridge ports on radios, and bridging functions such as address learning, packet forwarding, and Spanning Tree Protocol (STP).

Use of Radios for Backhaul

Each access point in a backhaul configuration must have two radios and be enrolled in the network. One of the radios operates in normal mode to serve downstream APs or clients. The other radio assumes the backhaul role (BP), relaying network traffic from clients or other APs through the backhaul arrangement up to the wired network. Each radio operates in a different band.

NOTE: The access point must have a wired connection to be enrolled in the network (see "Enrolling APs" on page 167). After the AP is enrolled, the wired connection can be removed.

For a backhaul point radio to establish a link with an AP, it must be able to receive its radio signals. Accordingly, the AP node with the BP radio must be within range of the upstream AP radio. A radio can be configured to operate in the BP mode even if its node is directly connected to the wired network, as in the case of building-to-building bridge applications.

From the perspective of the wired APs, each backhaul AP appears as a client; however, these "clients" are not identified in the RADIUS user database. For authentication purposes, identity information for the backhaul APs is automatically entered into the internal RADIUS database on the security services portal AP upon enrollment of the backhaul node. Users cannot view or modify this information.

Wireless Backhaul Trunks

A trunk is a wireless connection from one access point radio to another. An access point that is not connected to the wired network or an access point explicitly configured in the BP mode tries to establish a wireless trunk connection to another access point. A succession of trunks established between access points provides a path from client stations through the wireless network to the wired network.

If a trunk connection fails or a backhaul link goes down, then the access point that established the trunk re-scans the wireless environment and attempts to connect to another AP radio with compatible wireless and network characteristics. This process is called retrunking.

Backhaul retrunking usually occurs quickly (2-3 seconds) if uplink candidates are available. Subnets do not change as a result of retrunking. If a backhaul trunk fails and the BP radio cannot reestablish (recover) backhaul within 30 minutes, all backhaul links formed with its uplink AP radio are brought down. This gives an opportunity for the downlink nodes to attempt to form alternate backhaul paths.

Wireless Backhaul security

After enrollment, the BP radio uses WPA (EAP) for authentication and AES for encryption on its trunk or trunks. The following security restrictions apply:

- The upstream AP must have WPA enabled.
- All WPA-compatible authentication and encryption schemes are permitted.
- WEP may be enabled in addition to WPA on the upstream AP
- Both upstream and downstream APs must be enrolled by NM Portal.

For more information on security, see Chapter 7, "Managing Security."

Setting Up a Wireless Backhaul

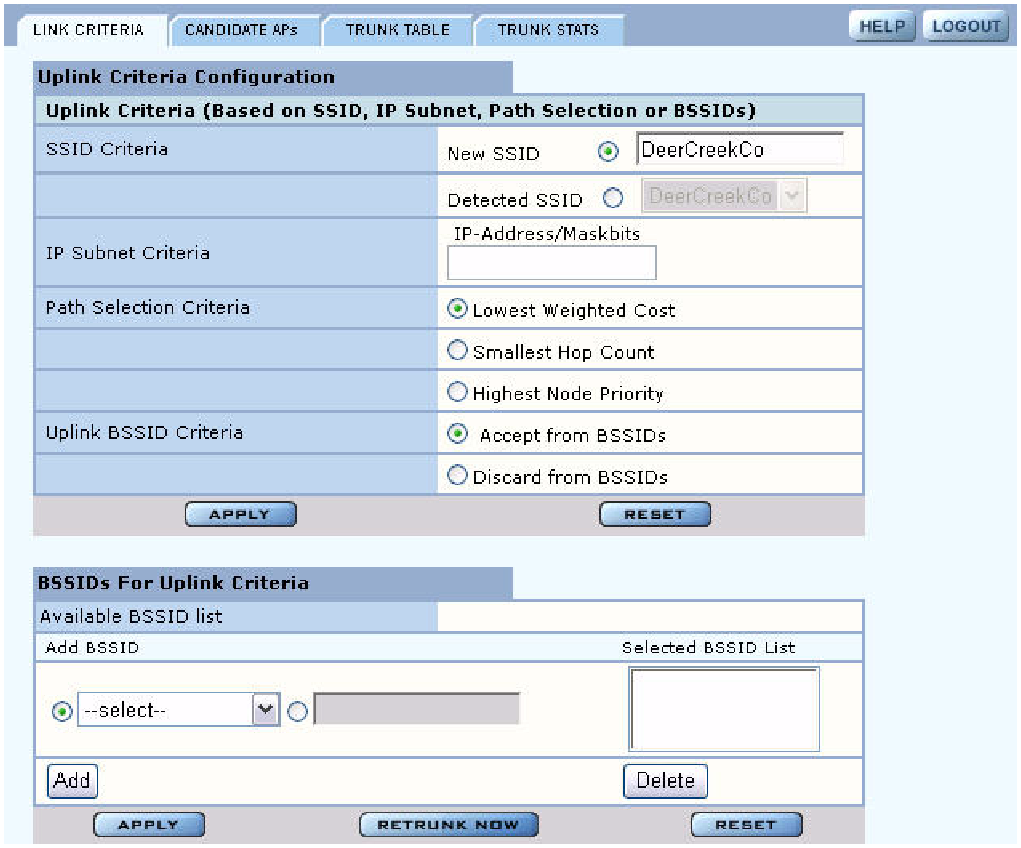
Choose **Wireless Backhaul** from the Wireless menu to bring up the Wireless Backhaul configuration panel. The panel contains 4 tabs:

- Link Criteria—Configure criteria for backhaul trunk formation.
- Candidate APs—Identify APs to use for the uplink.
- Trunk Table—View the list of current backhaul trunks.
- Trunk Stats—View statistics for the backhaul trunks.

Link Criteria

Use the Link Criteria tab (Figure 97) to set up the network parameters for the wireless backhaul. These parameters specify the rules that apply to the backhaul point (BP) radios which form uplink backhaul trunks by associating to normal radios (AP). These rules are used to determine the candidate parent list of upstream APs for the backhaul trunk.

Figure 97: Backhaul Configuration - Link Criteria



Uplink Criteria Configuration

Uplink Criteria (Based on SSID, IP Subnet, Path Selection or BSSIDs)	
SSID Criteria	New SSID ● DeerCreekCo
	Detected SSID ○ DeerCreekCo
IP Subnet Criteria	IP-Address/Maskbits
Path Selection Criteria	● Lowest Weighted Cost
	○ Smallest Hop Count
	○ Highest Node Priority
Uplink BSSID Criteria	● Accept from BSSIDs
	○ Discard from BSSIDs

BSSIDs For Uplink Criteria

Available BSSID list

Add BSSID: ● --select-- ○

Selected BSSID List

The Uplink Configuration settings on this tab restrict how the backhaul is configured. Select some or all of the settings, or leave this section blank to permit unrestricted choice of uplinks:

Field	Description
Select Radio Interface	Select radio wlan0 or wlan1.
SSID Criteria	Select Detected SSID to connect to a specific network. To add an SSID which is not currently in operation, select New SSID and enter the name of the SSID. This configuration is one of the attributes used by the radio in BP mode to form a backhaul.
IP Subnet Criteria	Enter an IP address and subnet prefix length to restrict the backhaul to a specific subnet. The BP radio selects those APs as candidates that advertise the specified subnet. If the IP address is 0.0.0.0, the BP radio ignores the subnet ID as a criterion when selecting AP candidates for trunk formation.
Path Selection Criteria	Choose the criterion for selecting the best wireless backhaul route from the following three options: • Lowest Weighted Cost—Candidate parent APs are selected in ascending order of path cost. (The candidate parent with lowest path cost to the wired network is the one with highest priority). Path cost is a cumulative metric in which each hop contributes to the path cost value. The calculation factors in the backhaul and non-backhaul traffic load on the candidate AP and quality of the link between the backhaul end points. • Smallest Hop Count—Candidate parents are selected in ascending order of hop count (number of hops to the wired network). • Highest Node priority—Candidate parents are selected in ascending order of priority as determined by the configured uplink BSSID list.
Uplink BSSID Criteria	This parameter is used in conjunction with the area entitled BSSIDs For Uplink Criteria at the bottom of the tab to restrict uplink candidates to a specific set of BSSIDs or to permit all BSSIDs except a designated list. • To restrict candidates to a designated list, select **Accept from BSSIDs**. • To avoid candidates on a specified list, select **Discard from BSSIDs**.

After making changes in the Uplink Criteria Configuration section, click **Apply**. Click **Reset** to return the parameters on the panel to the previous saved values.

Use the area at the bottom of the tab to specify the BSSID criteria (in conjunction with the Uplink BSSID buttons):

Field	Description
Add BSSID	To add BSSIDs to the Selected list, add from the pull-down list, and click **Add**. Alternatively, enter the name of a BSSID, and click **Add**. The saved BSSIDs are displayed in the selected BSSIDs list on the right. This list that determines acceptable uplink candidates (if Accept from BSSIDs was selected in Uplink BSSID Criteria), or eliminated uplink candidates (if Discard from BSSIDs was selected).

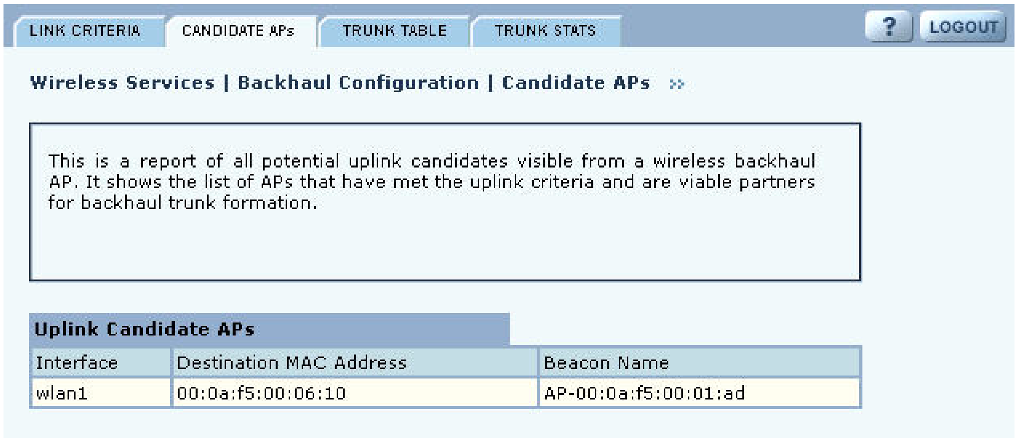
After adding BSSIDs, click **Apply**. The BP now attempts to establish a backhaul link based upon the configured rules.

Click **Delete** to remove a BSSID from the list.

Candidate APs

Select the Candidate APs tab (Figure 98) to identify the access points that can be used to create the uplink to the wired network.

Figure 98: Backhaul Configuration - Candidate APs



Wireless Services | Backhaul Configuration | Candidate APs

This is a report of all potential uplink candidates visible from a wireless backhaul AP. It shows the list of APs that have met the uplink criteria and are viable partners for backhaul trunk formation.

Uplink Candidate APs

Interface	Destination MAC Address	Beacon Name
wlan1	00:0a:f5:00:06:10	AP-00:0a:f5:00:01:ad

The panel displays the discovered APs that are able to provide uplink connectivity. The table of uplink candidate APs shows the following information:

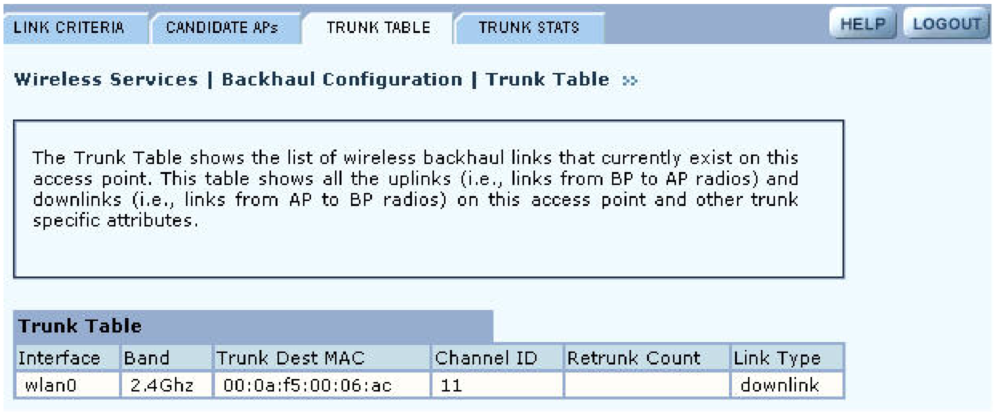
Feature	Description
Interface	Radio interface of uplink candidate parent
Destination MAC Address	BSSID of the remote uplink candidate parent
AP beacon name	Name of the AP node of the candidate parent, sent in beacons

If no uplink candidate APs are available, the table is empty.

Trunk Table

Select the Trunk Table tab (Figure 99) to view the list of current backhaul trunks. The backhaul is established if the MAC address of the backhaul trunk is listed in the table.

Figure 99: Backhaul Configuration - Trunk Table



Wireless Services | Backhaul Configuration | Trunk Table

The Trunk Table shows the list of wireless backhaul links that currently exist on this access point. This table shows all the uplinks (i.e., links from BP to AP radios) and downlinks (i.e., links from AP to BP radios) on this access point and other trunk specific attributes.

Trunk Table

Interface	Band	Trunk Dest MAC	Channel ID	Retrunk Count	Link Type
wlan0	2.4Ghz	00:0a:f5:00:06:ac	11		downlink

This tab contains the following information:

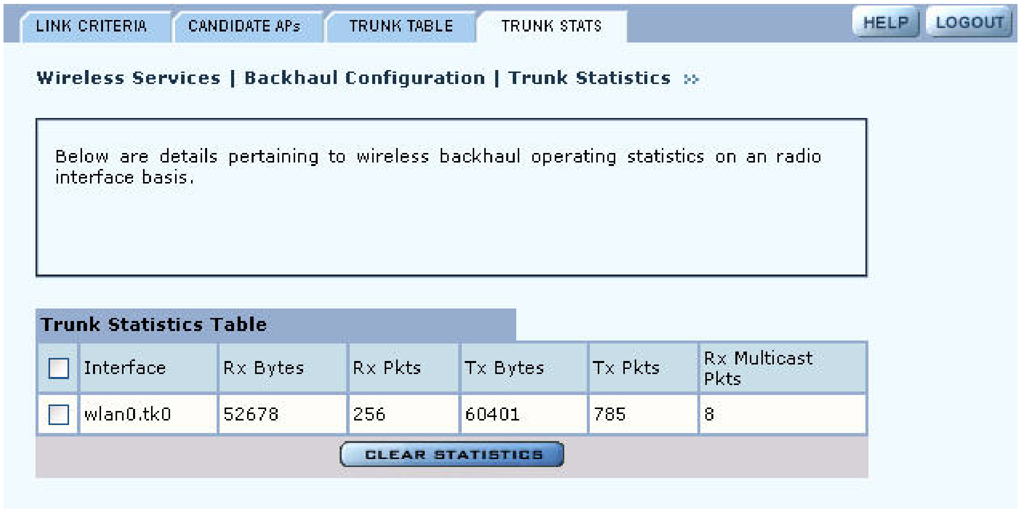
Feature	Description
Interface Name	Radio interface of the BP radio (uplink) or AP radio to which downlink trunks are connected. Applies to uplink and downlink trunks.
Band (2.4 GHz or 5 GHz, or both)	Operating band of the uplink or downlink trunks. Applies to uplink and downlink trunks. For the uplink trunk the band is the operating band of the BP radio. For downlink trunks the band is the operating band of the AP radio.
Trunk Dest MAC	MAC address (BSSID) of the remote backhaul destination. For Uplink trunks this is the MAC address of the parent AP; for downlink trunks it is the MAC address of the BPs (children) associated with the AP radio. Applies to uplink and downlink trunks.
Channel	ID of the channel on which the backhaul trunks (uplink and downlink) are operating. Applies to uplink and downlink trunks.
Re-trunk counts	Number of times the BP (uplink) retrunked (could be due to trunk failure or trunk optimization). Applies only to the uplink trunk.
Link Type	Indication of whether the interface is an uplink or downlink trunk

If no trunks are detected, the table is empty.

Trunk Statistics

Select the Trunk Statistics tab (Figure 100) to statistics for the available backhaul trunks. If no trunks are detected, the table is empty. To clear the cumulative statistics, click **Clear Statistics**.

Figure 100: Backhaul Configuration - Trunk Stats



Wireless Services | Backhaul Configuration | Trunk Statistics »

Below are details pertaining to wireless backhaul operating statistics on an radio interface basis.

Trunk Statistics Table

□	Interface	Rx Bytes	Rx Pkts	Tx Bytes	Tx Pkts	Rx Multicast Pkts
□	wlan0.tk0	52678	256	60401	785	8

This tab contains the following information:

Field	Description
Interface	The AP radio interface (wlan0 or wlan1)
Rx Bytes	Number of bytes received at this AP
Rx Packets	Number of packets received at this AP

Field	Description
Tx Bytes	Number of packets transmitted by this AP
Tx Packets	Number of packets transmitted by this AP
Rx Multicast Packets	Number of multicast packets received by this AP

Click **Clear Statistics** to return the counts in this tab to zero and begin collecting statistics again.

7 Managing Security

This chapter describes the encryption and authentication features of the 108 Mbps Wireless Access Point and explains how to set the security configuration. The chapter includes the following topics:

- **Introduction**
- **Configuring Wireless Security**
- **Configuring Authentication Zones**
- **Configuring Administrator Security**
- **Viewing Security Statistics**
- **Configuring Advanced Parameters**

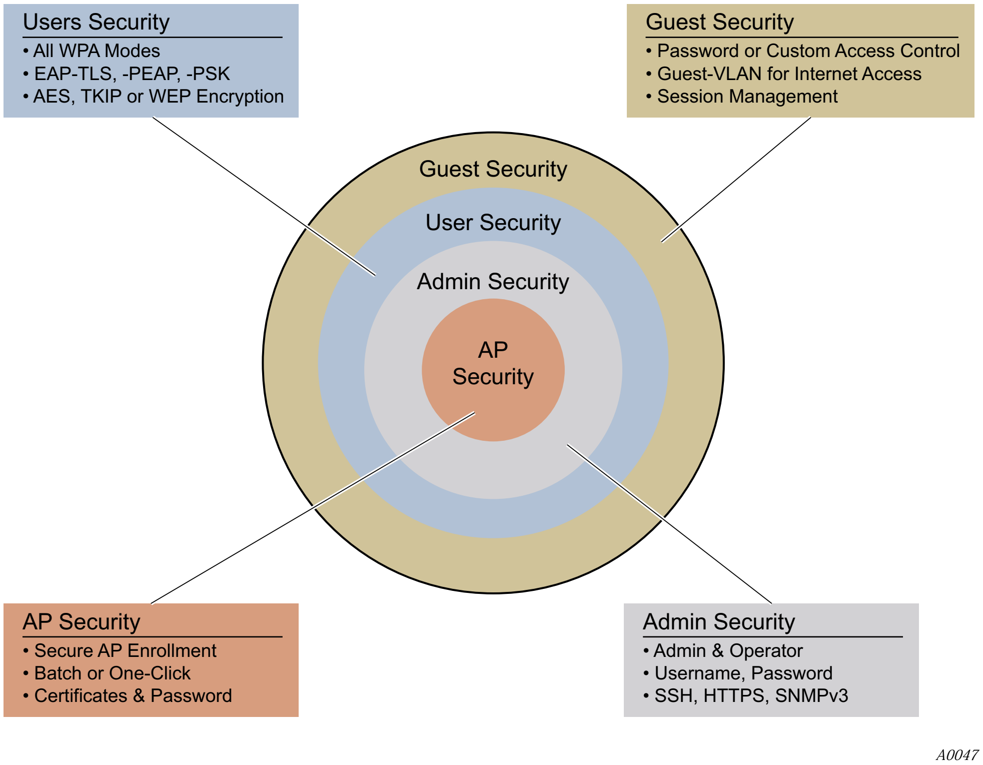
ℹ **NOTE:** For information on security for access point enrollment, refer to Chapter 9, "Managing the Network."

Introduction

PLANEX offers the strongest available security options for wireless networking, as listed here and illustrated in Figure 101:

- AP Security verifies the identity of individual APs and authorizes them to be part of the wireless network. APs can be enrolled individually or pre-enrolled as group. The process uses a certificate and password to fully verify the identity of the AP. By clearly identifying which APs belong to the authorized set, the enrollment process can also help identify unauthorized or rogue APs.
- Administrator security authorizes designated users to access the configuration and management capabilities of the AP using HTTPS, SSH, or SNMPv3 for the web interface, CLI, or network management system.
- User security encompasses authentication and encryption. Authentication verifies the identity of individual users and gives them access to the network, restricted to specific network service profiles. Once the network and authenticated users are in place, data encryption protects the privacy of user data transmitted over the wireless network.
- Guest access security provides password or custom access control for guest users, including the configuration of a guest-VLAN for Internet access and session management.

Figure 101: Elements of PLANEX Security



AP Security

PLANEX provides a highly secure process to enroll access points. Three distinct levels of identification verify the AP: Device ID, Thumbprint, and a bootstrap password unique to the AP. To assure central control of the verification process, it is recommended that a single enrollment server handle enrollment for the entire wireless network. The architecture supports two enrollment server options:

- AP Enrollment Server—Designate an NM Portal AP as the enrollment server for the network. For instructions, see Chapter 9, “Managing the Network.”
- Wireless LAN Network Management Software—The Wireless LAN Network Management Software network management system, offered as a separate product, operates as a complete enrollment solution for the enterprise. In addition to supporting manual AP enrollment, Wireless LAN Network Management Software includes automatic AP pre-enrollment by way of a bar code reader interface. For information on using Wireless LAN Network Management Software, see the *Wireless LAN Network Management Software Installation and Configuration Guide*.

Administrative Security

SSH, https, and SNMPv3 are used for secure administrative access to the AP.

User Security

Acceptable and effective solutions for user authentication depend upon the network size, complexity, and existing authentication infrastructure.

Current user authentication standards are based on the IEEE 802.1x specification, which identifies users and permits connectivity based upon policies established in a central server. Many authentication servers use the Remote Authentication Dial-In User Service (RADIUS) protocol, which enables remote access servers to communicate with the central server to authenticate users and authorize service or system access. Within the RADIUS context, the most effective authentication methods use versions of the Extensible Authentication Protocol (EAP) for the end-to-end authentication of the client by the authentication server.

The 108 Mbps Wireless AP can meet all the user authentication needs for the full range of wireless networks. (See Chapter 2, "Planning Your Installation.") PLANEX supports several modes of authentication, as listed in Table 11. WPA-PSK uses pre-shared keys (PSK) that is configured directly by the administrator into the AP and network clients. Based on the network wide key, the clients and AP receive unique session keys for each client session. This approach can be effective for small businesses for whom strong encryption is desired but a centralized authentication infrastructure is not available. EAP-TLS (EAP with Transport Layer Security) is a certificate-based authentication method based on the TLS protocol. The RADIUS security services within the 108 Mbps Wireless AP provide EAP-TLS for user authentication. PLANEX also supports integration with RADIUS servers that support EAP-TLS or EAP-PEAP.

In addition to the EAP-based authentication methods, PLANEX supports WEP-based encryption for legacy clients. PLANEX also supports the option of no user authentication.

Table 11: Authentication Options

Type	Description
EAP-TLS	Certificate-based authentication, used by the PLANEX security services portal and many external RADIUS servers
EAP-PEAP	EAP-PEAP RADIUS based authentication
WPA - PSK	Authentication acceptable for small to mid-size installations, in which manual distribution of keys is convenient and centralized management is not required
Dynamic WEP with 802.1x	Not recommended due to limitations of the WEP algorithms. If it is necessary to use this option to support legacy equipment, make sure that a RADIUS server configured for the SSID. The RADIUS server should be configured to support EAP-TLS or EAP-PEAP. Note that the 108Mbps Wireless LAN PC Card does not support dynamic WEP.
None	No user authentication

Data Encryption

Table 12 lists the available options for data encryption, in order of decreasing protection. The current standard for data encryption is WPA-AES, which provides financial-grade protection. The WEP encryption options use 64-bit or 128-bit encryption keys, assigned manually or dynamically, as dictated by the capabilities of the client. These offer some protection against casual interlopers; however, the WEP algorithms are vulnerable to compromise and can be difficult to maintain. WPA-TKIP closes the major WEP loopholes and can be an acceptable alternative to standard WEP.

Open encryption provides no protection, and is only recommended when security is not of concern. WPA-AES is recommended for all installations, if possible.

Table 12: Encryption Options

Type	Description
AES	Highest level of protection
TKIP	WEP with additional protection
WEP 128	First generation encryption using 128-bit keys, does not provide adequate protection
WEP 64	First generation encryption using 64-bit keys, does not provide adequate protection
Open	No protection

Configure and view the following aspects of network and user security from the web interface:

- Wireless Security—Select protocols for data encryption and user authentication.
- Authentication Zones—Group resources for user authentication.
- Administrator Security—Set the administrator login and password to access the AP.
- RADIUS Servers—Identify authorized RADIUS servers and zones.
- Security Statistics—View security-related statistics, including authentication, 802.1x supplicant, and authentication diagnostic statistics.
- Advanced—Configured advanced RADIUS properties.

Configuring Wireless Security

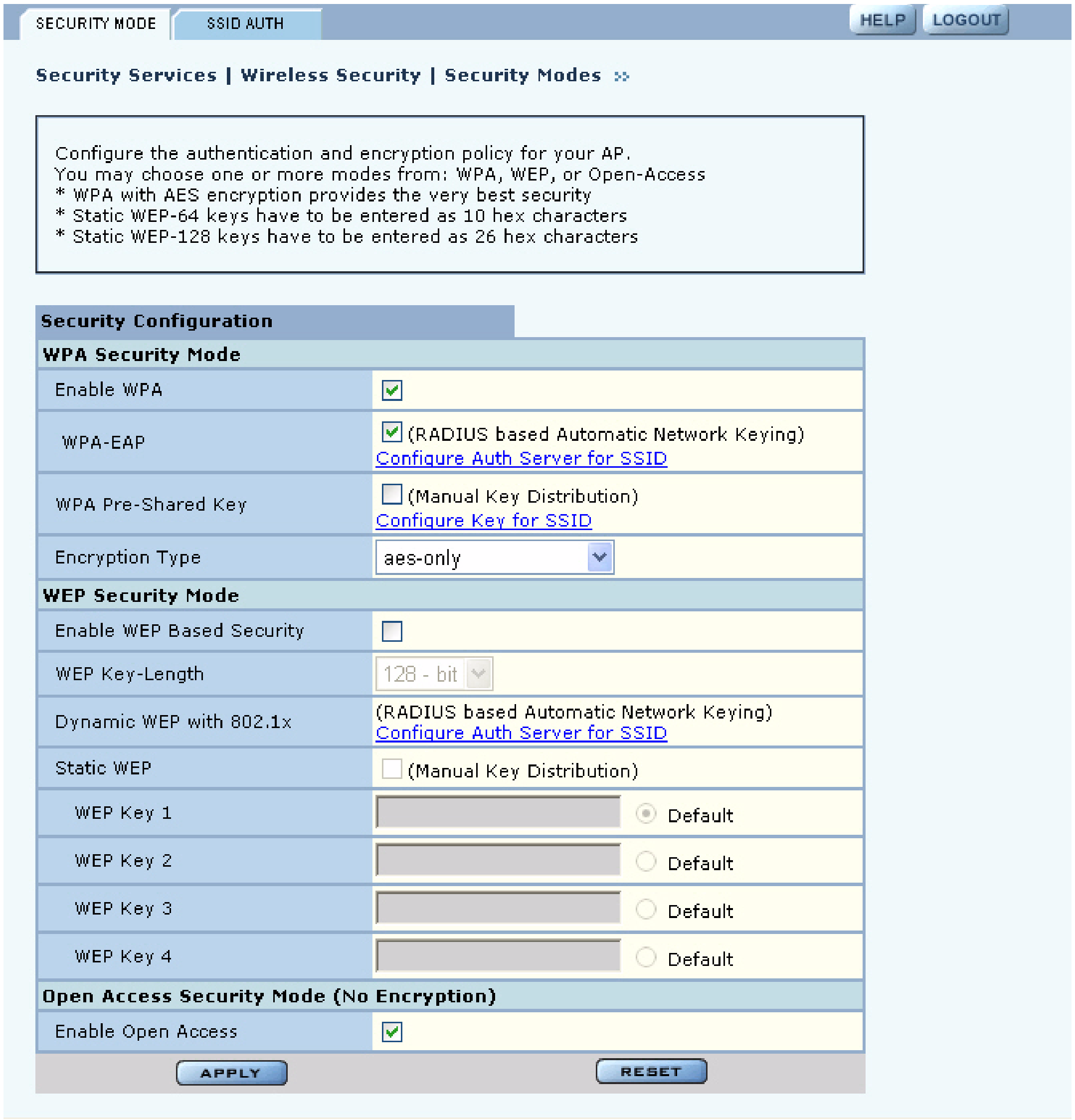
Choose **Wireless Security** from the Security Services menu to configure the protocols for data encryption and user authentication. The Wireless Security panel contains two tabs:

- Security Mode—Configure WPA, WEP, or open encryption and authentication.
- SSID Auth—Identify the authentication server for the SSID.

Security Mode

Use the Security Mode tab (Figure 102) to assign the encryption and authentication methods, including WPA, WEP, or Open. Allowing multiple encryption modes can be useful to support installations with a mixture of client wireless adapters. There are some limitations to the allowed combinations; it is not possible to enable both WEP and Open simultaneously. Also, Open and WPA encryption modes require each mode to be mapped to a separate VLAN (see “Configuring VLANs” on page 107).

Figure 102: Security Services - Security Mode



Security Services | Wireless Security | Security Modes »

Configure the authentication and encryption policy for your AP.
You may choose one or more modes from: WPA, WEP, or Open-Access
* WPA with AES encryption provides the very best security
* Static WEP-64 keys have to be entered as 10 hex characters
* Static WEP-128 keys have to be entered as 26 hex characters

Security Configuration

WPA Security Mode	
Enable WPA	☑
WPA-EAP	☑ (RADIUS based Automatic Network Keying) Configure Auth Server for SSID
WPA Pre-Shared Key	□ (Manual Key Distribution) Configure Key for SSID
Encryption Type	aes-only
WEP Security Mode	
Enable WEP Based Security	□
WEP Key-Length	128 - bit
Dynamic WEP with 802.1x	(RADIUS based Automatic Network Keying) Configure Auth Server for SSID
Static WEP	□ (Manual Key Distribution)
WEP Key 1	● Default
WEP Key 2	○ Default
WEP Key 3	○ Default
WEP Key 4	○ Default
Open Access Security Mode (No Encryption)	
Enable Open Access	☑

WPA Security

Select **Enable WPA** to activate the WPA authentication and encryption fields. The following options are available:

Field	Description
WPA Security Mode	WPA-EAP—For RADIUS-based networking keying WPA-PSK—For pre-shared keys
Encryption Type	AES, TKIP, AES and TKIP

Click **Apply** to save the configuration, or **Reset** to return to the previously saved values.

WPA provides strong encryption support with the AES and TKIP algorithms.

NOTE: Some early versions of WPA-capable client software may not permit a client to associate to the AP when multiple modes off encryption and authentication are chosen.

NOTE: Selecting WPA-EAP or WPA-PSK displays a link that leads to the SSID Authentication tab. Refer to "SSID Authentication" on page 142 for instructions on using this tab.

WEP Security

If it is necessary to configure WEP security, select **Enable WEP** to activate the WEP fields. Configure the following values in the WEP security area:

Field	Description
Enable WEP	Activate the WEP settings. The 108 Mbps Wireless AP supports WEP with dynamic and manually entered keys. To use dynamic keys, select WEP, but do not enter values in the Key fields.
Key-Length	Select 64-bit or 128-bit
Key 1 - Key 4	For manual keys, enter up to four WEP key values. Each WEP key is 26 hex-ASCII characters. (required if security mode is WEP)

Click **Apply** to save the settings or **Reset** to clear the fields on the panel.

Open Access

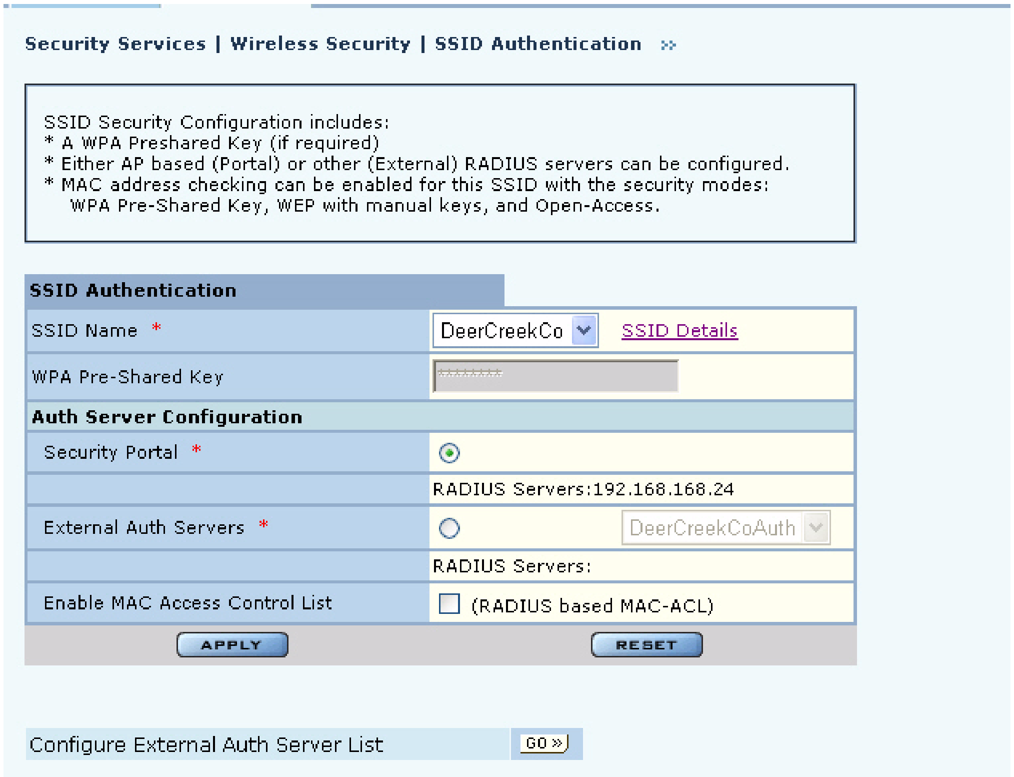
Select **Enable Open Access** to omit data encryption. A pop-up message warns of the potential security risk in using open access. Click **OK** to continue.

SSID Authentication

Use the SSID Authentication tab (Figure 103) to assign RADIUS Authentication servers or a WPA pre-shared key. RADIUS based authentication uses lists of servers, called authentication zones, which are provided by the 108 Mbps Wireless AP security portal or an external RADIUS server. Each SSID can be configured with the RADIUS servers used for EAP authentication and the WPA pre-shared key (if applicable).

MAC-ACL lookups can be enabled for clients that associate with WPA-PSK, manual WEP-keys, or with no security. MAC-ACL is not applicable if per user authentication is done where user name is available.

Figure 103: Security Services - SSID Auth



Security Services | Wireless Security | SSID Authentication »

SSID Security Configuration includes:
* A WPA Preshared Key (if required)
* Either AP based (Portal) or other (External) RADIUS servers can be configured.
* MAC address checking can be enabled for this SSID with the security modes:
  WPA Pre-Shared Key, WEP with manual keys, and Open-Access.

SSID Authentication	
SSID Name *	DeerCreekCo SSID Details
WPA Pre-Shared Key	********
Auth Server Configuration	
Security Portal *	●
	RADIUS Servers:192.168.168.24
External Auth Servers *	○ DeerCreekCoAuth
	RADIUS Servers:
Enable MAC Access Control List	□ (RADIUS based MAC-ACL)

Assign the following values to configure SSID authentication:

Feature	Description
SSID Name	Select from the SSID pull-down list. Click **SSID Details** to view more SSID-related information, enable multiple SSIDs, or change other SSID attributes.
WPA Pre-Shared Key	Enter the pre-shared key for WPA, if appropriate. This field is grayed out if WPA-PSK is not the selected authentication type.
Authentication Server Configuration	Select the Security Portal or External Authentication Server radio button. For Security Portal, the IP addresses of all security portals are displayed below the radio button. For External security, select from the list of RADIUS servers or click **Go** at the bottom of the tab to configure the authentication server list (see “Authentication Zones” on page 145). (required)
Enable MAC Access Control List	Select to enable authentication using MAC addresses that are centrally managed in a RADIUS server. For MAC-ACL authentication, it is necessary to use a security portal or external RADIUS server.

Click **Apply** to save changes or **Reset** to return to previously saved values. It may be necessary to click **Back** on your browser to return to the Security Configuration panel. Make sure to also click **Apply** on the Security Configuration panel.

An external RADIUS server can also be added from this tab. Click **Go** at the bottom of the tab to open the Authentication Zone tab of the Authentication Zones panel. For instructions on adding a server, refer to “Configuring Authentication Zones” on page 145.

If an external RADIUS server is to be used for MAC address based ACL lookups, the following apply:

1 The RADIUS server must have PAP authentication enabled for these MAC ACL users

2 The RADIUS server can expect the AP to send the following standard RADIUS attributes in the authentication request for purposes of policy configuration and interoperability. (MAC addresses must be in sent with no colon or hyphen separators):

Attribute	Description
User-Name	MAC address
User-Password	MAC address
Message-Authenticator	RADIUS extension providing enhanced authentication of message contents. (This is the same as the signature attribute in some RADIUS servers).
NAS-IP-Address	Management IP address of the AP
NAS-Port	Radio interface number for the associating station
NAS-Port-Type	Standard value Wireless - IEEE 802.11. Indicates that the user has requested access via an 802.11 port on the AP.

3 The RADIUS server should enforce a policy such that MAC ACL users are only allowed to use PAP authentication for Wireless. This is important because the username and password are not secret.

4 The RADIUS server may optionally send back the Session-Timeout attribute to override the AP default session-timeout.

5 The RADIUS server may optionally send back an attribute encoded with the user group.

If an external RADIUS server is used for EAP based authentication (with WPA or with legacy 802.1x), the following information should be used when configuring the server:

1 The RADIUS server can expect the AP to send the following standard RADIUS attributes in the authentication request for purposes of policy configuration and interoperability:

Attribute	Description
User-Name	Contains the MAC address in the format specified above.
EAP-Message	Contains the EAP messages received from the station.
Framed-MTU	Contains a hint to help the RADIUS server for EAP fragmentation
Message-Authenticator	The RADIUS extension that provides enhanced authentication of the message contents. (Also referred to as signature attribute in some RADIUS servers).
NAS-IP-Address	Contains the management IP address of the AP.
NAS-Port	Contains the radio interface number on which the station is associating.
NAS-Port-Type	Contains the standard value “Wireless - IEEE 802.11” to indicate that the user to be authenticated has requested access via an 802.11 port on the AP.

2 The RADIUS server can use these attributes to enforce policies such that EAP based authentication is mandatory for Wireless.

3 The RADIUS server may optionally send back the “Session-Timeout” attribute to override the AP default session-timeout.

4 The RADIUS server may optionally send back an attribute encoded with the user group.

Configuring Authentication Zones

RADIUS servers may be used to authenticate wireless users and administrative users, and to check MAC Access Control Lists for the SSID.

Select **Authentication Zones** from the Security Services menu to define zones for RADIUS authentication and to add external RADIUS servers to the list of available authentication servers. Configure the servers first, and then include them in zones.

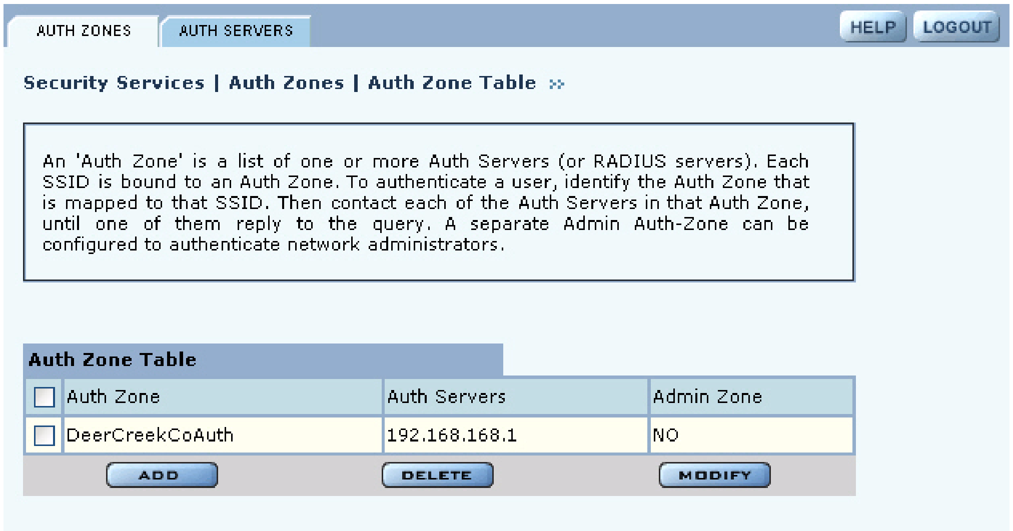
The Authentication Zone panel contains two tabs:

- Auth Zones—Define zones for RADIUS authentication.
- Auth Servers—Add RADIUS servers.

Authentication Zones

On the Authentication Zones tab (Figure 104), you can create new authentication zones or modify existing ones. Select check boxes for authentication zones you want to modify or delete, or click **Add** to add a new zone.

Figure 104: Authentication Zones - Auth Zones



An 'Auth Zone' is a list of one or more Auth Servers (or RADIUS servers). Each SSID is bound to an Auth Zone. To authenticate a user, identify the Auth Zone that is mapped to that SSID. Then contact each of the Auth Servers in that Auth Zone, until one of them reply to the query. A separate Admin Auth-Zone can be configured to authenticate network administrators.

Auth Zone Table

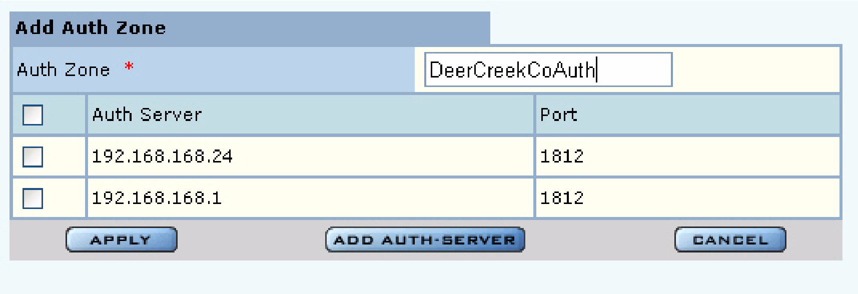
□	Auth Zone	Auth Servers	Admin Zone
□	DeerCreekCoAuth	192.168.168.1	NO

Set the following values on the Add Auth Zone entry panel (Figure 105):

Field	Description
Auth Zone	Name of the authentication zone.
Auth Server list	List of possible servers to add to the zone. Select desired servers.

Click **Add** after making selections.

Figure 105: Authentication Zones - Add Auth Zones



Add Auth Zone

Auth Zone *	DeerCreekCoAuth	
□	Auth Server	Port
□	192.168.168.24	1812
□	192.168.168.1	1812

To add a new authentication server, click **Add Auth-Server**, and enter the following values for each new RADIUS server:

Field	Description
Auth Server	IP address of the RADIUS authentication server.
Shared Secret	Enter and confirm the secret key.
Port Number	Port number for the server (default is 1812).

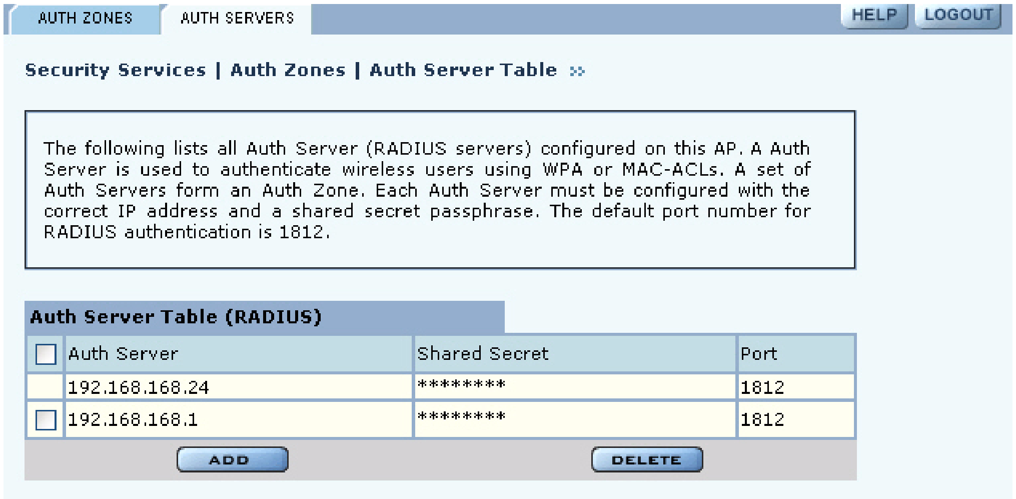
Click **Add** to save the values, or click **Reset** to clear the fields on the panel.

Click **Back** on your browser to return to the Auth Zone panel. Set an authentication zone for administrative users by selecting from the pull-down list.

Authentication Servers

Open the Authentication Servers tab (Figure 106) to view the current authentication servers and add or delete servers.This table shows the list of both internal (security portals) and external auth servers. The servers that do not have a check box against them are security portals.

Figure 106: Authentication Zones - Auth Servers



Security Services | Auth Zones | Auth Server Table »

The following lists all Auth Server (RADIUS servers) configured on this AP. A Auth Server is used to authenticate wireless users using WPA or MAC-ACLs. A set of Auth Servers form an Auth Zone. Each Auth Server must be configured with the correct IP address and a shared secret passphrase. The default port number for RADIUS authentication is 1812.

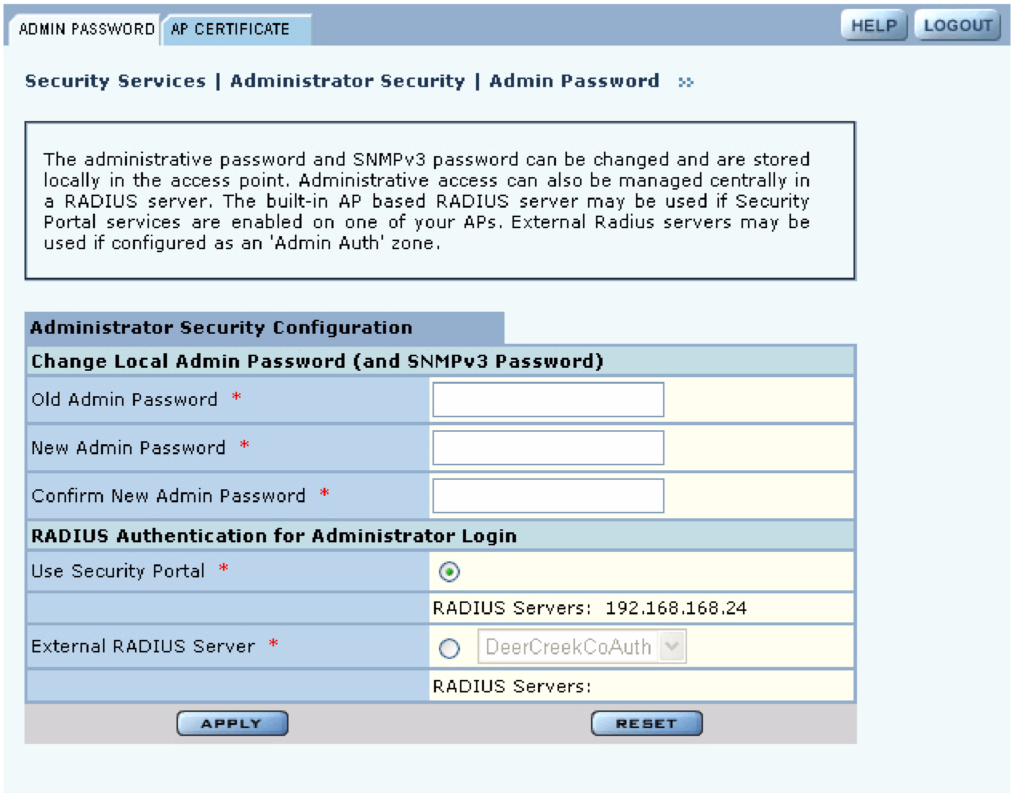
Auth Server Table (RADIUS)

□	Auth Server	Shared Secret	Port
	192.168.168.24	********	1812
□	192.168.168.1	********	1812

Configuring Administrator Security

Choose **Administrator Security** from the Security Services menu to open the Administrator Security panel (Figure 107).

Figure 107: Administrator Security - Admin Password



Security Services | Administrator Security | Admin Password

The administrative password and SNMPv3 password can be changed and are stored locally in the access point. Administrative access can also be managed centrally in a RADIUS server. The built-in AP based RADIUS server may be used if Security Portal services are enabled on one of your APs. External Radius servers may be used if configured as an 'Admin Auth' zone.

Administrator Security Configuration

Change Local Admin Password (and SNMPv3 Password)	
Old Admin Password *	
New Admin Password *	
Confirm New Admin Password *	
RADIUS Authentication for Administrator Login	
Use Security Portal *	●
	RADIUS Servers: 192.168.168.24
External RADIUS Server *	○ DeerCreekCoAuth
	RADIUS Servers:

Set the following values on this panel:

Field	**Description**
Change Local Admin Password	Enter the old password and the new password, and confirm the new password. This password is used for the local administrative login and the SNMPv3 administrative login. (required)
RADIUS Authentication for Network Administrator Login	Select whether to use the Portal AP security feature for network administrator authentication or use an external RADIUS server. With the external RADIUS server option, links are available to add, delete, or edit the list of servers. (required)

Click **Apply** to save the settings or **Reset** to clear the fields on the panel.

External RADIUS Server Settings

The following rules apply for an external RADIUS server:

- The external RADIUS server must have Password Authentication Procedure (PAP) authentication enabled for administrative users.
- The 108 Mbps Wireless AP sends a standard RADIUS attribute called “Service-Type” in the authentication request. The value of this attribute is set to “Administrative” to indicate that the user to be authenticated has requested access to an administrative interface on the AP
- If the user authentication is successful, the RADIUS server must send back an PLANEX vendor-specific attribute defined as follows:

  `vendor-id=13586, vendor sub-type=3, integer value = 1.`

This attribute informs the AP that the user is not normal user, but rather an administrator who may be granted access to the privileged administrative interface.

Viewing Security Statistics

Choose **Security Statistics** item from the menu tree to open the Security Statistics panels. This panel contains the following tabs:

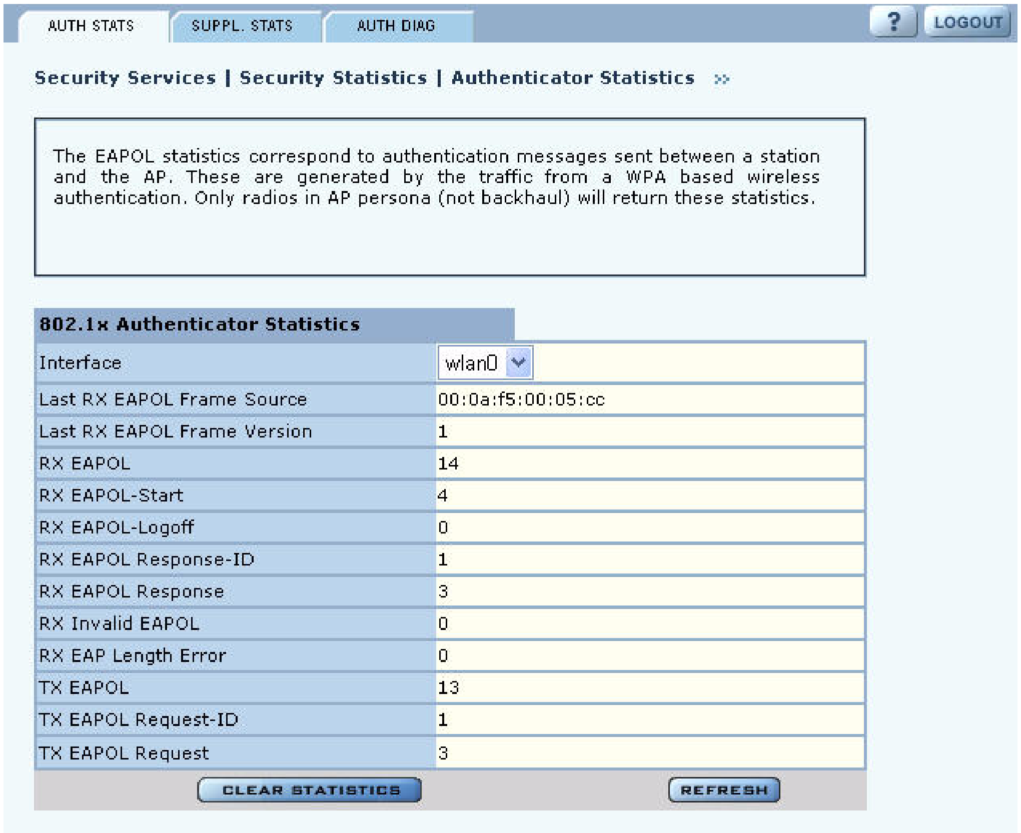
- Auth Stats—View authentication statistics for each selected AP radio.
- Suppl Stats (Supplicant Statistics)—View statistics on 802.1x requests, for each selected BP radio.
- Auth Diag—View authentication diagnostics statistics, including back-end data.

Each of the tabs includes a Reset button to return the statistics to zero and begin collecting them again.

Authentication Statistics

The Authentication Statistics tab (Figure 108) contains EAPOL statistics, which correspond to authentication messages sent between a station and an AP. These are generated by the traffic from WPA or 8021.x based wireless authentication. Only radios in AP mode produce this data.

Figure 108: Security Statistics - Authentication Stats


AUTH STATS
SUPPL. STATS
AUTH DIAG
?
LOGOUT
Security Services | Security Statistics | Authenticator Statistics >>

The EAPOL statistics correspond to authentication messages sent between a station and the AP. These are generated by the traffic from a WPA based wireless authentication. Only radios in AP persona (not backhaul) will return these statistics.

802.1x Authenticator Statistics	
Interface	wlan0
Last RX EAPOL Frame Source	00:0a:f5:00:05:cc
Last RX EAPOL Frame Version	1
RX EAPOL	14
RX EAPOL-Start	4
RX EAPOL-Logoff	0
RX EAPOL Response-ID	1
RX EAPOL Response	3
RX Invalid EAPOL	0
RX EAP Length Error	0
TX EAPOL	13
TX EAPOL Request-ID	1
TX EAPOL Request	3

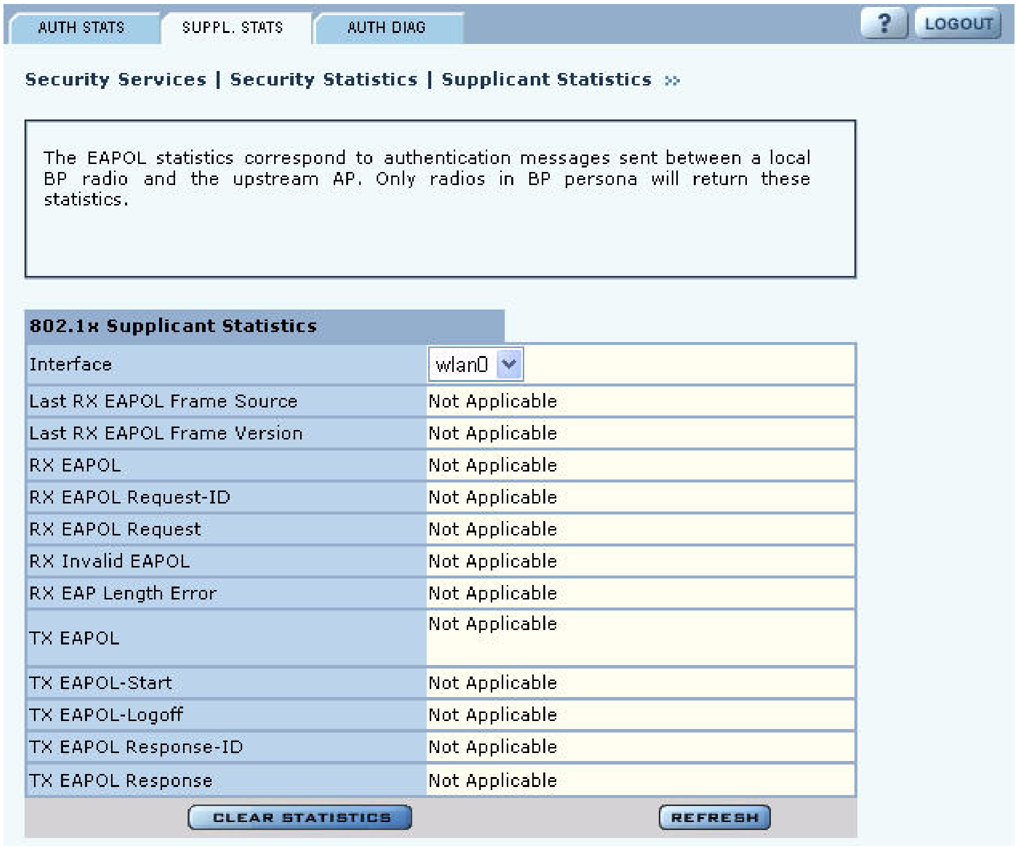
The tab contains the following information:

Field	Description
Interface	Select the radio interface of interest for viewing statistics.
Last RX EAPOL Frame Source	The source MAC address from the last EAPOL frame received by the AP. This identifies a station or BP that is currently authenticating or re-authenticating with the AP.
Last RX EAPOL Frame Version	The EAPOL version from the last EAPOL frame received by the AP.
RX EAPOL	The total number of EAPOL frames received by the AP.
RX EAPOL-Start	The total number of EAPOL-Start frames received by the AP. This count increments as stations or BPs request the AP to start their authentication sequence.
RX EAPOL-Logoff	The total number of EAPOL-Logoff frames received by the AP. This count may not increment as most 802.1x peers do not send this frame for security reasons.
RX EAPOL Response-ID	The total number of EAPOL based EAP Response-ID frames received by the AP. This count increments as stations or BPs present their user-id or device-id information to the AP at the start of the authentication sequence.
RX EAPOL Response	The total number of EAPOL based EAP Response frames received by the AP that do not contain an EAP Response-ID. This count increments as the AP receives authentication credentials derived from passwords or certificates from stations or BPs that are authenticating with it.
RX Invalid EAPOL	The total number of EAPOL frames received by the AP that have invalid packet type fields. These frames are discarded by the AP.
RX EAP Length Error	The total number of EAPOL frames received by the AP that have invalid packet body length fields. These frames are discarded by the AP.
TX EAPOL	The total number of EAPOL frames transmitted by this AP.
TX EAPOL Request-ID	The total number of EAPOL based EAP Request-ID frames transmitted by this AP. This count increments as the AP sends authentication frames to stations or BPs requesting them to return their user-id or device-id information at the very start of the authentication sequence.
TX EAPOL Request	The total number of EAPOL based EAP Request frames transmitted by the AP that do not contain an EAP Request-ID. This count increments as the AP transmits authentication credentials derived from passwords or certificates to the stations or BPs that are authenticating with it.

Supplicant Statistics

The Supplicant Stats tab(Figure 109) reports on authentication messages sent between a local BP radio and the upstream AP. Only radios in BP mode return these statistics. The statistics are generated from the EAPOL protocol, which is used for 802.1x authentication.

Figure 109: Security Statistics - Supplicant Stats


AUTH STATS
SUPPL. STATS
AUTH DIAG
?
LOGOUT
Security Services | Security Statistics | Supplicant Statistics »
CLEAR STATISTICS
REFRESH

The EAPOL statistics correspond to authentication messages sent between a local BP radio and the upstream AP. Only radios in BP persona will return these statistics.

802.1x Supplicant Statistics	
Interface	wlan0
Last RX EAPOL Frame Source	Not Applicable
Last RX EAPOL Frame Version	Not Applicable
RX EAPOL	Not Applicable
RX EAPOL Request-ID	Not Applicable
RX EAPOL Request	Not Applicable
RX Invalid EAPOL	Not Applicable
RX EAP Length Error	Not Applicable
TX EAPOL	Not Applicable
TX EAPOL-Start	Not Applicable
TX EAPOL-Logoff	Not Applicable
TX EAPOL Response-ID	Not Applicable
TX EAPOL Response	Not Applicable

The tab contains the following information:

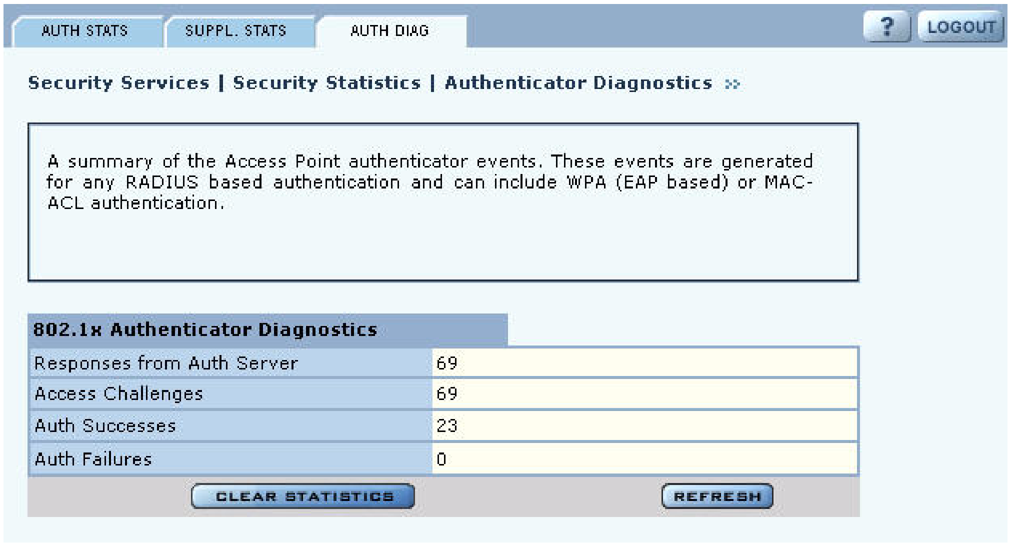
Field	Description
Interface	Select the radio interface of interest for viewing statistics.
Last RX EAPOL Frame Source	The source MAC address from the last EAPOL frame received by the BP. This identifies the upstream AP that is currently authenticating or re-authenticating with the BP.
Last RX EAPOL Frame Version	The EAPOL version from the last EAPOL frame received by the BP.
RX EAPOL	The total number of EAPOL frames received by the BP.
RX EAPOL Request-ID	The total number of EAPOL based EAP Request-ID frames received by this BP. This count increments as the AP sends authentication frames to the BP requesting it to its device-id information at the very start of the authentication sequence.
RX EAPOL Request	The total number of EAPOL based EAP Request frames received by the BP that do not contain an EAP Request-ID. This count increments as the AP transmits authentication credentials derived from certificates to the BP.
RX Invalid EAPOL	The total number of EAPOL frames received by the BP that have invalid packet type fields. These frames are discarded by the BP.
RX EAP Length Error	The total number of EAPOL frames received by the BP that have invalid packet body length fields. These frames are discarded by the BP.

Field	Description
TX EAPOL	The total number of EAPOL frames transmitted by this BP.
TX EAPOL-Start	The total number of EAPOL-Start frames transmitted by the BP. This count goes up as the BP requests the AP to start its authentication sequence.
TX EAPOL-Logoff	The total number of EAPOL-Logoff frames transmitted by the BP. This count will not increment as the BP does not send this 8021.x frame for security reasons.
TX EAPOL Response-ID	The total number of EAPOL based EAP Response-ID frames transmitted by this BP. This count increments as the BP sends authentication frames to the AP with its device-id information at the very start of the authentication sequence.
TX EAPOL Response	The total number of EAPOL based EAP Response frames transmitted by the BP that do not contain an EAP Response-ID. This count increments as the BP transmits authentication credentials derived certificates to the AP that is authenticating with it.

Authentication Diagnostics

The Authentication Diagnostics tab (Figure 110) contains a summary of the Access Point authenticator events received from a backend authentication server. These events are generated for any RADIUS based authentication and can include WPA (EAP based) or MAC-ACL authentication.

Figure 110: Security Statistics - Authentication Diagnostics



Security Services | Security Statistics | Authenticator Diagnostics >>

A summary of the Access Point authenticator events. These events are generated for any RADIUS based authentication and can include WPA (EAP based) or MAC-ACL authentication.

802.1x Authenticator Diagnostics	
Responses from Auth Server	69
Access Challenges	69
Auth Successes	23
Auth Failures	0

The tab contains the following information:

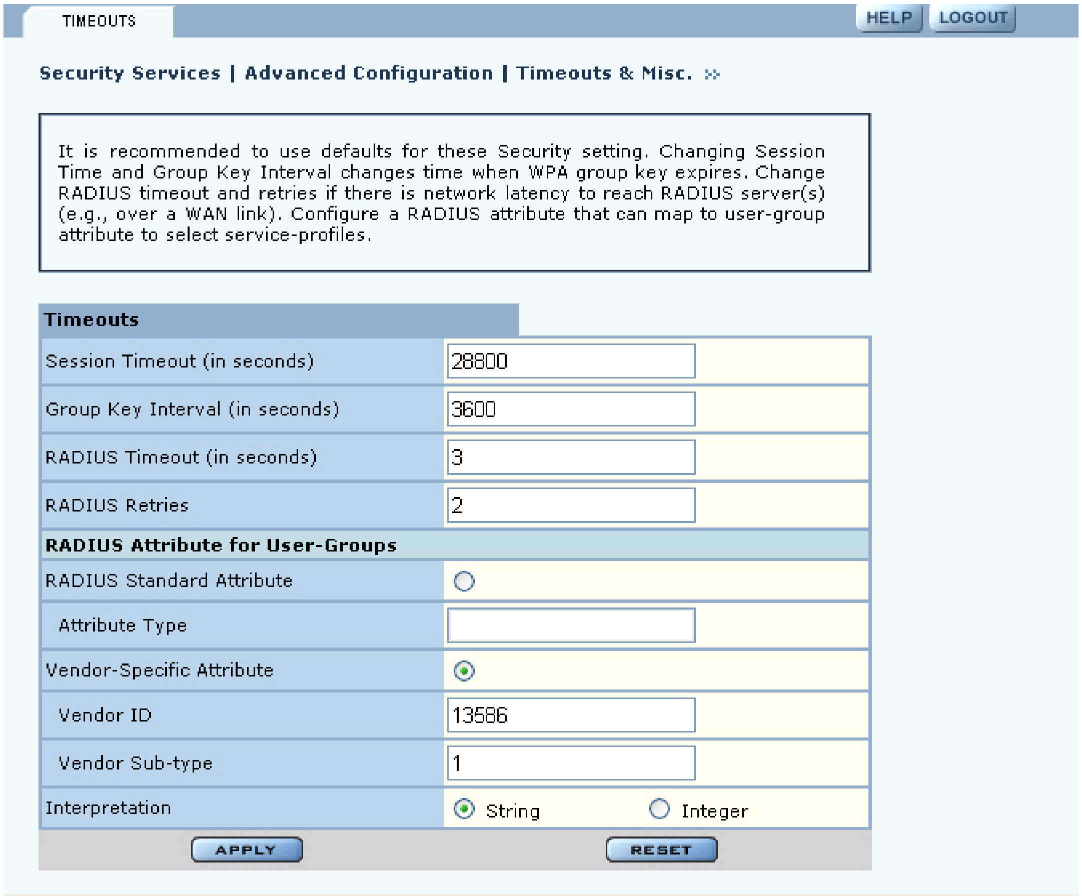
Field	Description
Responses from Auth Server	The total number of RADIUS authentication related packets received from the backend authentication server.
Access Challenges	The total number of RADIUS authentication packets that contained an ACCESS-CHALLENGE. These are sent by the RADIUS server when it is engaged in a multi-step authentication sequence.

Field	Description
Auth Successes	The total number of RADIUS authentication packets that contained an ACCESS-ACCEPT. These are sent by the RADIUS server when the authentication sequence succeeds.
Auth Failures	The total number of RADIUS authentication packets that contained an ACCESS-REJECT. These are sent by the RADIUS server when the authentication sequence fails.

Configuring Advanced Parameters

Choose **Advanced Configuration** from the menu tree to open the Advanced RADIUS configuration panel (Figure 111). It is not necessary to modify any of the settings on this panel.

Figure 111: Advanced Configuration - Timeouts



TIMEOUTS
HELP
LOGOUT
Security Services | Advanced Configuration | Timeouts & Misc.

It is recommended to use defaults for these Security setting. Changing Session Time and Group Key Interval changes time when WPA group key expires. Change RADIUS timeout and retries if there is network latency to reach RADIUS server(s) (e.g., over a WAN link). Configure a RADIUS attribute that can map to user-group attribute to select service-profiles.

Timeouts	
Session Timeout (in seconds)	28800
Group Key Interval (in seconds)	3600
RADIUS Timeout (in seconds)	3
RADIUS Retries	2
RADIUS Attribute for User-Groups	
RADIUS Standard Attribute	○
Attribute Type	
Vendor-Specific Attribute	●
Vendor ID	13586
Vendor Sub-type	1
Interpretation	● String ○ Integer

The panel contains the following fields:

Field	Description
Session Timeout	Time in seconds, after which a station is re-authenticated
Group Key Interval	Time in seconds, after which the group key is changed. This is not used if static WEP keys are enforced
RADIUS Timeout	Time in seconds, after which the request is retransmitted

Field	Description
RADIUS Retries	Number of retransmit attempts, after which the RADIUS request is marked a failure.
External RADIUS Group-Key Attribute (for User Group ID)	RADIUS attribute used by the AP to determine the user group (see “SSID Details” on page 83). When a wireless user is authenticated by a RADIUS server, the server can optionally send the AP the ‘User Group’ for the association. If a user group is not returned, then the user is not assigned a group, and the user gets the default service profile for the SSID. By default, a Vendor Specific Attribute is used (13586, 1, String).

Other standard or vendor specific attributes can be used to determine service policies. For example, an enterprise having an existing RADIUS attribute for VLANs can reuse the attributes for AP service profile assignments by configuring them as the RADIUS attributes for user groups.

Click **Apply** to implement the changes, or click **Reset** to return the entries on the panel to their previous values.

8 Configuring Guest Access

This chapter describes how to enable guest user access to the wireless network while protecting the network from unauthorized use. It contains the following sections:

- **Overview**
- **Configuring Guest Access**
- **Guest Access Services Panel**

Overview

Guest access can be used to allow visitors to a facility to access the Internet through the wireless network without gaining access to the corporate network. Most current guest user solutions require guests to access a separate access point that is not part of the corporate network. The PLANEX solution eliminates this requirement by restricting guest access through VLAN tags on the existing access points. There is no need to set up special access points or to physically restrict the locations used for guest access.

Unauthenticated users are permitted to associate to an AP, but any web communications are captured and directed to a controlled landing page, the “captive portal.” The landing page allows the guest user to login using a web-based password scheme. The page can inform unauthenticated users of the network access policies and provide instructions on obtaining the guest password. Following successful authentication, the guest user is released from the captive pages and allowed to access any resource on the guest VLAN.

The VLAN configuration of the upstream network should make available only those network resources set aside for guest use. This often means prohibiting guest stations from accessing anything other than the corporate open subnet or the Internet.

For open guest access, the open access security option must be configured. This precludes the use of WEP Security Mode on APs that provide guest access, but does permit use of WPA Security Mode.

VLANs and security privileges are assigned to users by way of service profiles defined for user groups and bound to the network SSID. It is required that the VLAN configuration include DHCP and DNS services.

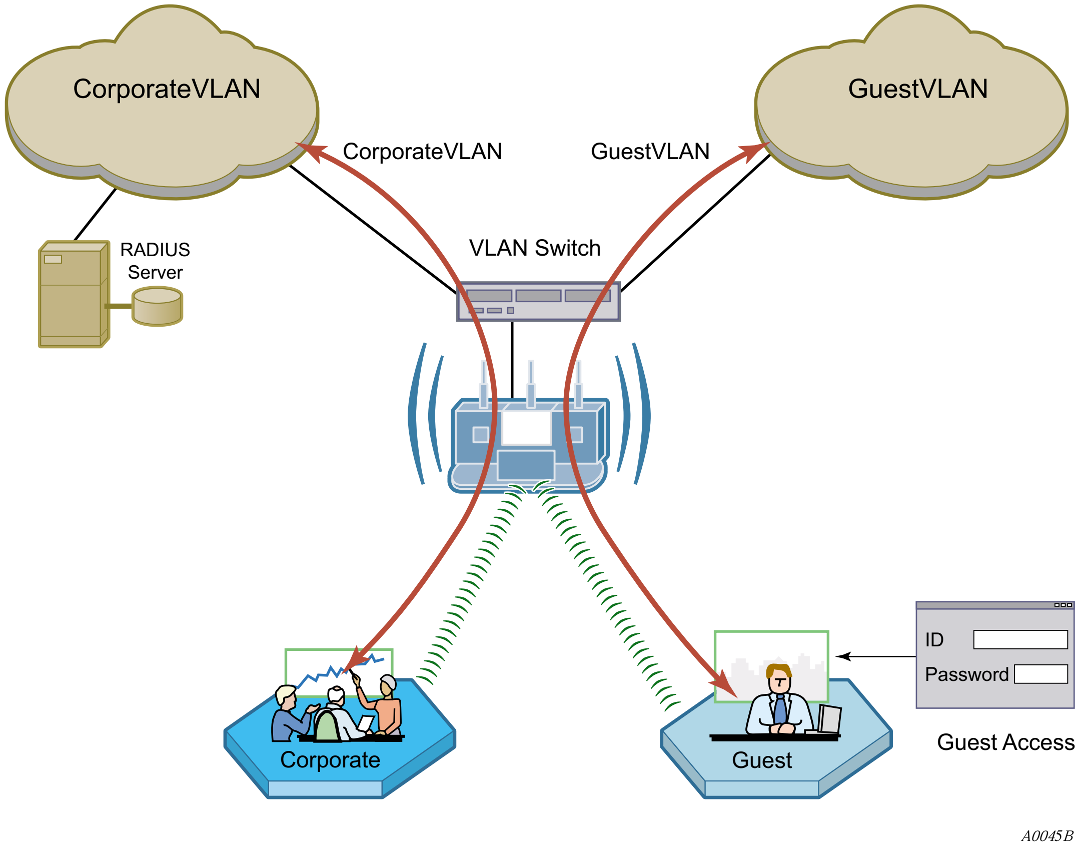
Guest user authentication can be implemented using an internal or external landing page.

Internal Landing Page

The internal landing page is a configurable option within the 108 Mbps Wireless AP. The guest password for the AP can be set using the Guest Access panel, or an automatically generated password can be configured through the User Management panel in NM Portal. If the automatically generated guest password is used, then the authentication process for the internal landing page also checks the password entered by the guest user against the RADIUS authentication service provided in the PLANEX security portal. If either password is acceptable, the guest user is authenticated and receives the privileges specified in the guest service profile.

Figure 112 shows how Acme Works configured guest access with an internal guest landing page. The company has two VLANs: Corporate and Guest. Corporate and guest users belong to the Enterprise and Guest user groups, respectively, with appropriate service profiles assigned and bound to the SSID. Corporate users are authenticated by way of the enterprise RADIUS server, while guest users are authenticated by way of an internal landing page configured in the 108 Mbps Wireless AP. After they are authenticated, guest users are place in the Guest VLAN.

Figure 112: Guest Access - Internal Landing Page

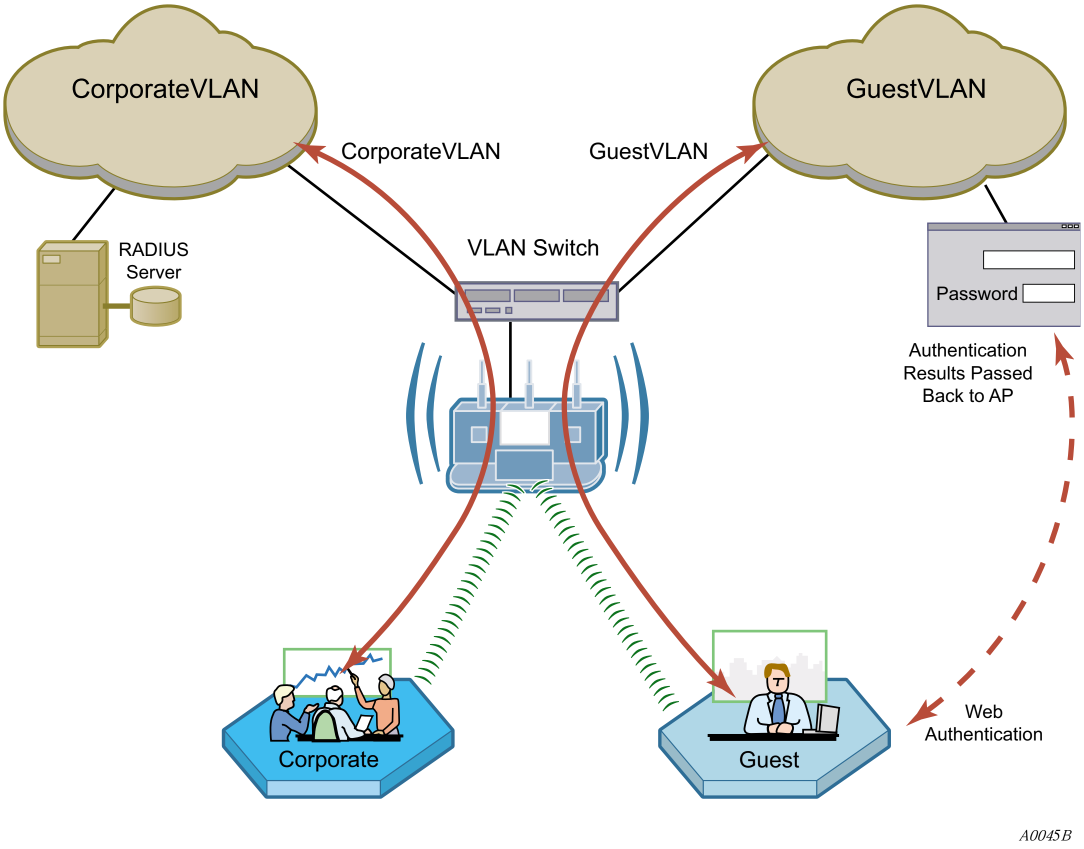


External Landing Page

An external landing web page can be set up through a corporate web server. The URL for the landing page must use an IP address rather than a domain name. Regardless of the authentication process selected for the external page, it is necessary to forward authentication results to the AP upon completion of successful or unsuccessful guest authentication.[1]

Figure 113 shows a network configuration with an external guest landing page. The external landing page is made accessible over the Internet through an external web server. As in the previous example, authenticated guest users are given access to the guest VLAN.

Figure 113: Guest Access - External Landing Page

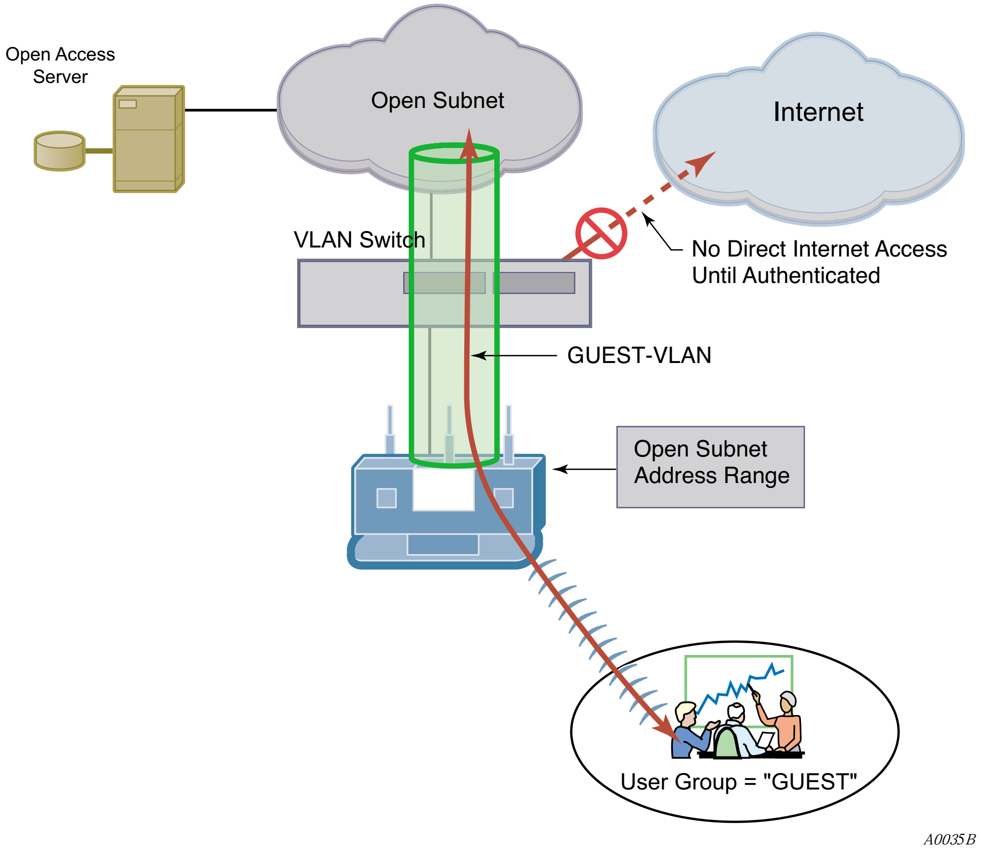


[1] An example external landing page is shipped with the 108 Mbps Wireless Access Point.

Open Subnet

In an optional open subnet arrangement, shown in Figure 114, unauthenticated guest users are permitted limited access to an open enterprise subnet specified in the 108 Mbps Wireless AP. The enterprise open subnet must be part of the Guest VLAN. Extended access requires authentication through an internal or external landing page.

Figure 114: Guest Access - Open Subnet



Configuring Guest Access

This section describes the complete process of setting up guest access. A Guest Access wizard is also available for easy configuration of the major guest access parameters. See “Guest Access Wizard” on page 50 for instructions on using the Guest Access wizard.

Task	Steps
Confirm that open access is supported as a security option.	1 Choose **Wireless Security** from the **Security Services** menu to open the Security Mode tab (“Configuring Wireless Security” on page 140). 2 Enable WPA security, if mixed mode security (encrypted and open) is desired. Only WPA can be enabled in conjunction with open. The WPA Security mode is for non-guests only. 3 Enable Open Access. 4 Click **Apply**.

Task (continued)	**Steps**
Create or confirm existence of a corporate VLAN. This can be the default untagged VLAN or a specially created VLAN.	**1** Choose **VLAN Configuration** from the **Networking Services** menu to open the VLAN table ("VLAN Table" on page 108). **2** Confirm that the corporate VLAN is listed in the table, or click **Add** to create a new VLAN: **a** Enter the corporate VLAN name and a numeric VLAN ID in the Add VLAN entry panel. **b** Enter the IP address and maskbits of the captive portal server, or select the DHCP option. The guest portal must have a valid IP address for the authentication process to work. **c** Select the eth0 interface, and mark it as tagged. (Only eth0 should be tagged.) **d** Click **Add**.
Create the guest VLAN.	**1** Choose **VLAN Configuration** from the **Networking Services** menu to open the VLAN table ("VLAN Table" on page 108). **2** Click **Add**. **3** Enter the VLAN name (Guest VLAN) and a numeric VLAN ID in the Add VLAN entry panel. It is not recommended to use the default VLAN. **4** Enter the IP address and maskbits of the captive portal server, or select the DHCP option. **5** Select the eth0 interface, and mark it as tagged. (Only eth0 should be tagged.) **6** Click **Add**. For additional information on configuring VLANS, see "Configuring VLANs" on page 107.
Create or confirm definition of a corporate service profile.	**1** Choose **SSID Configuration** from the **Wireless Services** menu to open the SSID table ("SSIDs and Service Profiles" on page 80). **2** Click **Profile Table**. **3** Add a corporate profile, or confirm that one exists with the desired WPA security option and the corporate VLAN specified. Make sure that the corporate profile is bound to the SSID.
Create a guest service profile which specifies the guest VLAN and desired COS and security options.	**1** Choose **SSID Configuration** from the **Wireless Services** menu to open the SSID table. **2** Select **SSID Details** ("SSID Details" on page 83). **3** Confirm the SSID name, or enter a new SSID name for the Guest Portal, and then click **Apply**. **4** Click **Profile Table** to display the current list of service profiles. **5** Click **Add** to create the guest service profile. Select the VLAN ID for the guest VLAN previously defined. Enter the COS value and make sure that no-encryption is selected. **6** Click **Apply**.

Task (continued)	Steps
Add guest access to the SSID and specify an internal or external landing page for guest users who attempt to access the network.	**1** Choose **Guest Access Configuration** from the Guest Access Services menu to open the Guest table. **2** Click **Add**. **3** Confirm selection of the SSID and guest profile, as defined in the previous task. **4** Select whether the landing page will be internal or external. If external, enter a URL and an external web server secret code, which is the shared secret code for communication between the AP and web server. **5** Click **Apply**.
For the internal landing page, set a guest password; for an external landing page use the RADIUS shared secret code.	**1** If Internal is selected as the landing page type, click **Security** to enter the guest password. **2** Enter and confirm the password, and then click **Apply**.
Set up optional auto-generation of guest passwords	**1** From NM Portal (Network Management Explorer) window, select **User Management** from the Security Portal menu. **2** On the Guest User tab (Figure 117), select **Yes** to enable auto-password generation. **3** Select an interval from the Generate Auto Guest Password pull-down list. **4** Click **Apply**. **NOTE:** If static and auto-generated passwords are configured, then a guest user can enter either password to be authenticated.

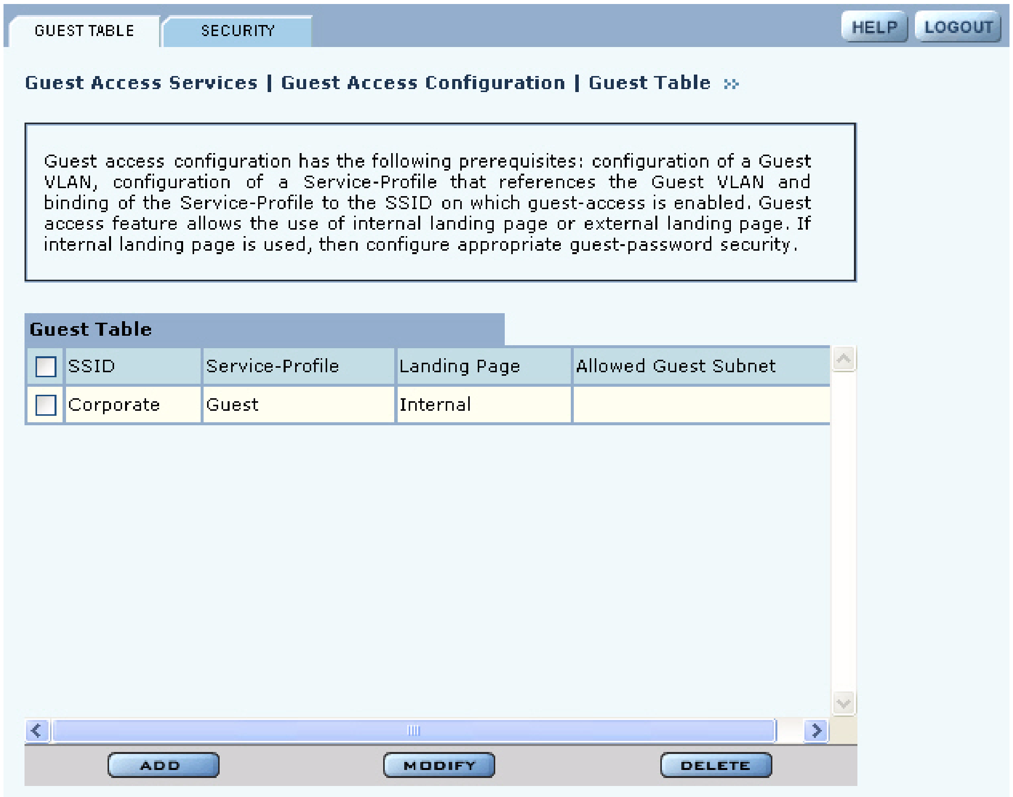
Guest access is now configured. When guests attempt to access the network, they are directed to an external landing page or to a standard user login screen. Upon entering the correct guest password or server secret code, they are granted access to the guest VLAN. They are also given the COS and encryption characteristics specified in the guest service profile.

Guest Access Services Panel

For summary information about guest access, use the Guest Access Configuration panel. The panel opens to the Guest table (Figure 115), which lists currently defined guest service profiles. The table presents the following information:

Field	Description
SSID	The network to which the guest profile belongs. There can be at most one guest profile per SSID.
Service-Profile	The name of the guest service profile bound to the SSID
Landing Page	Internal or external page automatically displayed when guest users attempt to access the network
Allowed Guest Subnet	The subnet optionally reserved for unauthenticated guest access. Configuring an allowed guest subnet can give unauthenticated users access to a limited set of free services.

Figure 115: Guest Access Configuration - Guest Table



Guest Access Services | Guest Access Configuration | Guest Table

Guest access configuration has the following prerequisites: configuration of a Guest VLAN, configuration of a Service-Profile that references the Guest VLAN and binding of the Service-Profile to the SSID on which guest-access is enabled. Guest access feature allows the use of internal landing page or external landing page. If internal landing page is used, then configure appropriate guest-password security.

Guest Table

□ SSID	Service-Profile	Landing Page	Allowed Guest Subnet
□ Corporate	Guest	Internal	

Perform the following functions from the Guest Table:

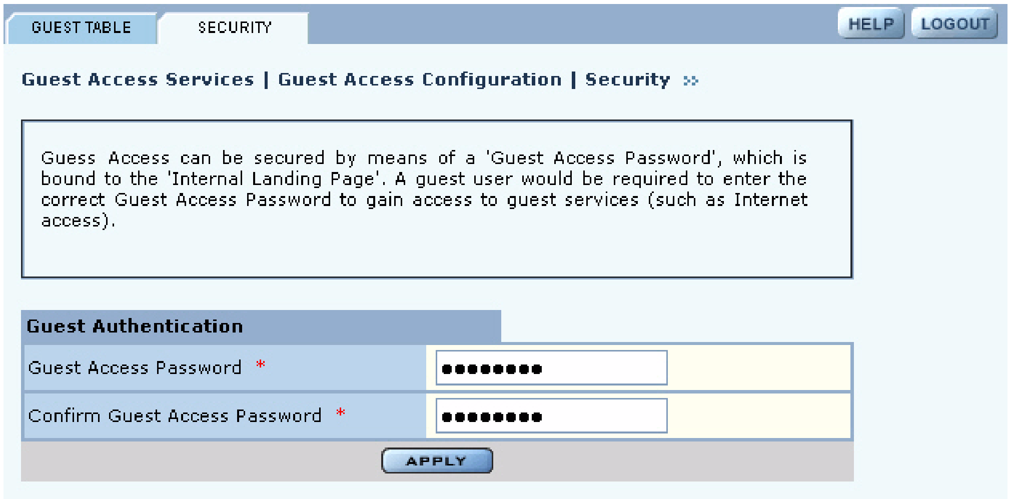
Function	Description
Add an entry to the Guest Table	One guest profile can be added for each SSID. If a profile is already assigned to an SSID and you add a new one, it replaces the previously defined profile. 1 Click **Add**. 2 Select the SSID. 3 Select the service profile from the Profile pull-down list. 4 If desired, enter the address and maskbits for a subnet optionally reserved for unauthenticated guest access. 5 Select an internal or external landing page. If the external page is selected, enter the full URL and the shared secret code used for communicating with the RADIUS server. 6 Click **Apply**.
Modify an entry	1 Select the entry you wish to modify, and click **Modify**. 2 Confirm the SSID. 3 Select the service profile from the Profile pull-down list. 4 If desired, enter the address and maskbits for a subnet optionally reserved for unauthenticated guest access. 5 Select an internal or external landing page. If the external page is selected, enter the full URL and shared secret code for access. Click **Apply**.

Function	Description
Delete an entry	**6** Select the entry and click **Delete**. **7** Click **OK** to confirm.

Guest Access Security

The Security tab of the Guest Access Configuration panel (Figure 116) provides an interface to set the guest password for an internal landing page.

Figure 116: Guest Access Configuration - Security


GUEST TABLE
SECURITY
HELP
LOGOUT
Guest Access Services | Guest Access Configuration | Security »

Guess Access can be secured by means of a 'Guest Access Password', which is bound to the 'Internal Landing Page'. A guest user would be required to enter the correct Guest Access Password to gain access to guest services (such as Internet access).

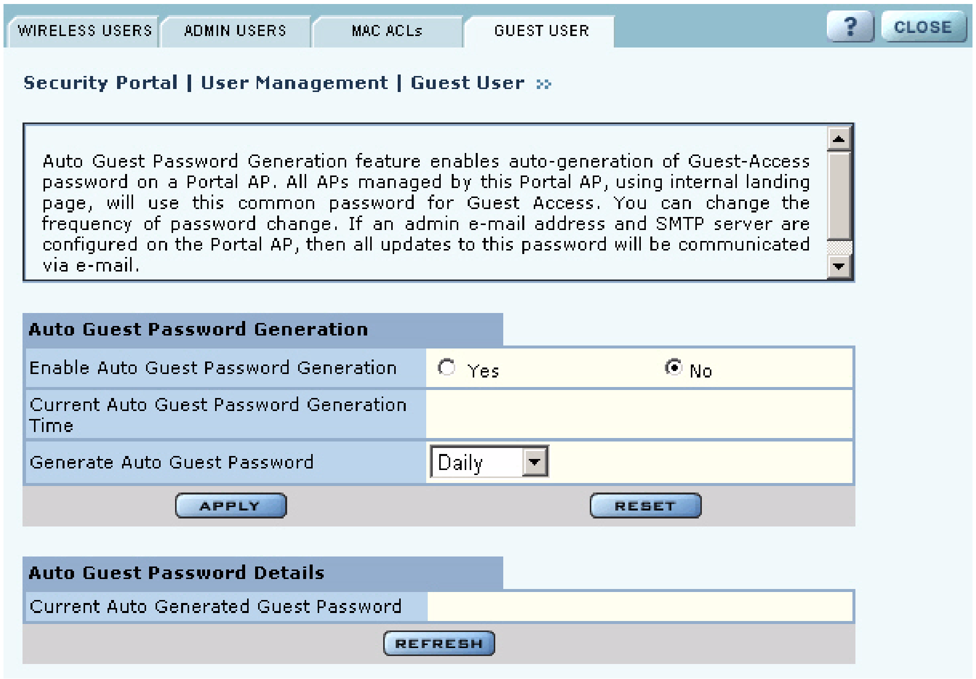
Guest Authentication

Guest Access Password *	●●●●●●●●
Confirm Guest Access Password *	●●●●●●●●

Auto-Generating Guest Passwords

For optional generation of guest passwords automatically at set intervals, use the Guest User tab within the security area of NM Portal (Figure 117).

Figure 117: Security Portal - Guest User



Security Portal | User Management | Guest User

Auto Guest Password Generation feature enables auto-generation of Guest-Access password on a Portal AP. All APs managed by this Portal AP, using internal landing page, will use this common password for Guest Access. You can change the frequency of password change. If an admin e-mail address and SMTP server are configured on the Portal AP, then all updates to this password will be communicated via e-mail.

Auto Guest Password Generation

Enable Auto Guest Password Generation	○ Yes ● No
Current Auto Guest Password Generation Time	
Generate Auto Guest Password	Daily

Auto Guest Password Details

Current Auto Generated Guest Password	

9 Managing the Network

This chapter explains how to use the NM Portal features of the 108 Mbps Wireless Access Point to manage multiple APs across the network. It includes the following topics:

- **Introduction**
- **Using NM Portal**
- **Using the Network Topology Menu**
- **Managing Rogue Access Points**
- **Using the NM Services Menu**
- **Managing Network Faults**
- **Managing Users**

Introduction

Network management refers to the coordinated control and supervision of multiple access points across a network. Network management functions include single-point configuration of multiple access points, user access control, performance monitoring, and fault management.

PLANEX offers the unique advantage of a network management capability built into the 108 Mbps Wireless Access Point. When configured as an NM Portal, the 108 Mbps Wireless AP can provide network management services for up to five subnetworks**.** For small to mid-size networks, this eliminates the need for an external network management application. For mid to large size enterprise networks, NM Portal can be used to manage all the APs at a specific location or branch, while Wireless LAN Network Management Software, offered as a separate product, can supply enterprise-level network management.

NM Portal supports the following functions:

- Single view to manage the entire network
- AP discovery
- AP enrollment
- Centralized software distribution and policy management
- Integrated security management for users
- Rogue AP control
- Email alerts
- Fault management
- Syslog
- Guest access control

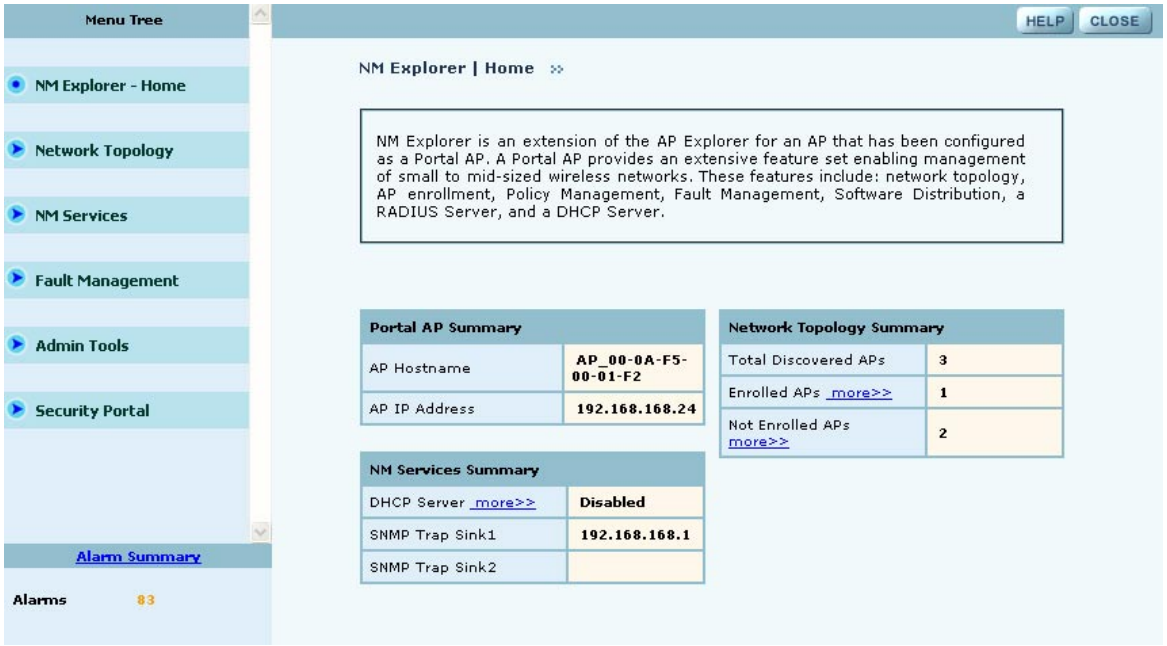
Using NM Portal

To use the 108 Mbps Wireless AP for NM Portal services, it is necessary to initialize (bootstrap) the unit in NM Portal mode. Do so when initially configuring the AP, or by resetting the AP to factory defaults prior to booting. Chapter 3, "Installing the Access Point," explains how to initialize an NM Portal and how to reset to factory defaults.

NOTE: Before resetting the AP to factory defaults, make sure to have the original password shipped with the unit available.

After the AP is initialized as a portal, access NM Portal services from the web interface at any time by clicking **Manage Wireless Network** on the menu tree or on the Home panel ("The Home Panel" on page 37). The NM Portal Network Management Explorer opens in a new browser window (Figure 118).

Figure 118: NM Portal Web Interface



NM Explorer | Home »

NM Explorer is an extension of the AP Explorer for an AP that has been configured as a Portal AP. A Portal AP provides an extensive feature set enabling management of small to mid-sized wireless networks. These features include: network topology, AP enrollment, Policy Management, Fault Management, Software Distribution, a RADIUS Server, and a DHCP Server.

Portal AP Summary	
AP Hostname	AP_00-0A-F5-00-01-F2
AP IP Address	192.168.168.24

NM Services Summary	
DHCP Server more>>	Disabled
SNMP Trap Sink1	192.168.168.1
SNMP Trap Sink2	

Network Topology Summary	
Total Discovered APs	3
Enrolled APs more>>	1
Not Enrolled APs more>>	2

Alarms 83

This interface is similar to that of the standard 108 Mbps Wireless AP web interface. The menu tree on the left contains a set of menus to access application features. Use the detail panels on the right to set the configuration and monitor the state of the network. The alarm panel in the lower left portion of the window shows the number of outstanding critical alarms collected across the NM Portal managed network.

Home Panel

The Home panel (Figure 118) contains summary information about the network configuration together with links to some of the Detail panels. Open the Home panel at any time by selecting **Home** from the menu tree.

Menu Tree

The menu tree contains the following menus:

- Home—Open the Home panel.

- Network Topology—Manage AP enrollment, wireless backhaul, IP address status, and radio neighbors.
- NM Services—Set up network discovery, DHCP settings, and portal settings.
- Fault Management—View alarm logs and syslog events.
- Admin Tools—Upgrade AP software (see “Upgrading Software” on page 221).
- Security Portal—Add network, administrative, and legacy users.

Each of these topics is described in this chapter, except Software Upgrade, which is described in Chapter 10, “Maintaining the Access Point.”

Click the arrow to the left of a menu item to expand the menu.

Using the Network Topology Menu

Use the Network Topology menu items to manage the identification, network status, and relationship of APs in the network.

Enrolling APs

Network security depends upon mutual trust between the NM Portal and the other managed 108 Mbps Wireless APs. Each access point must trust the identity of the NM Portal AP, and the NM Portal must trust that each access point is fully authenticated (Figure 119). Enrollment is the process used to establish this mutual trust. The process consists of several steps:

- NM Portal automatically discovers all the 108 Mbps Wireless Access Points and presents those that are not already enrolled in a list of unenrolled APs.
- You select a candidate AP to enroll and verify its identity.
- NM Portal and the AP perform a mutual authentication process.
- Once the authentication is complete, the AP is enrolled. It is not necessary to enroll the AP again, even if power is lost to the unit.

NOTE: In order to enroll an AP, it must be in the factory default state. This assures that enrollment will be based on a known configuration.

You can enroll up to 20 APs. To access the enrollment panel, choose **AP Enrollment** from the Network Topology menu. The AP Enrollment panel opens to display the list of discovered, but as yet un-enrolled, APs (Figure 120).

Figure 119: AP Enrollment

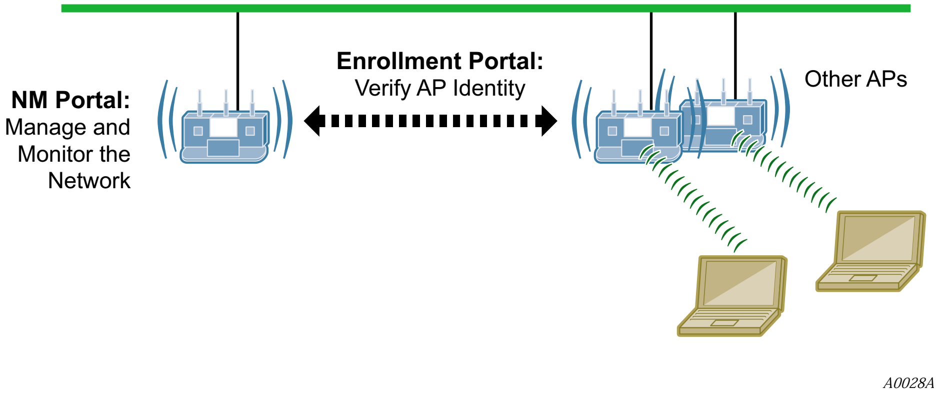
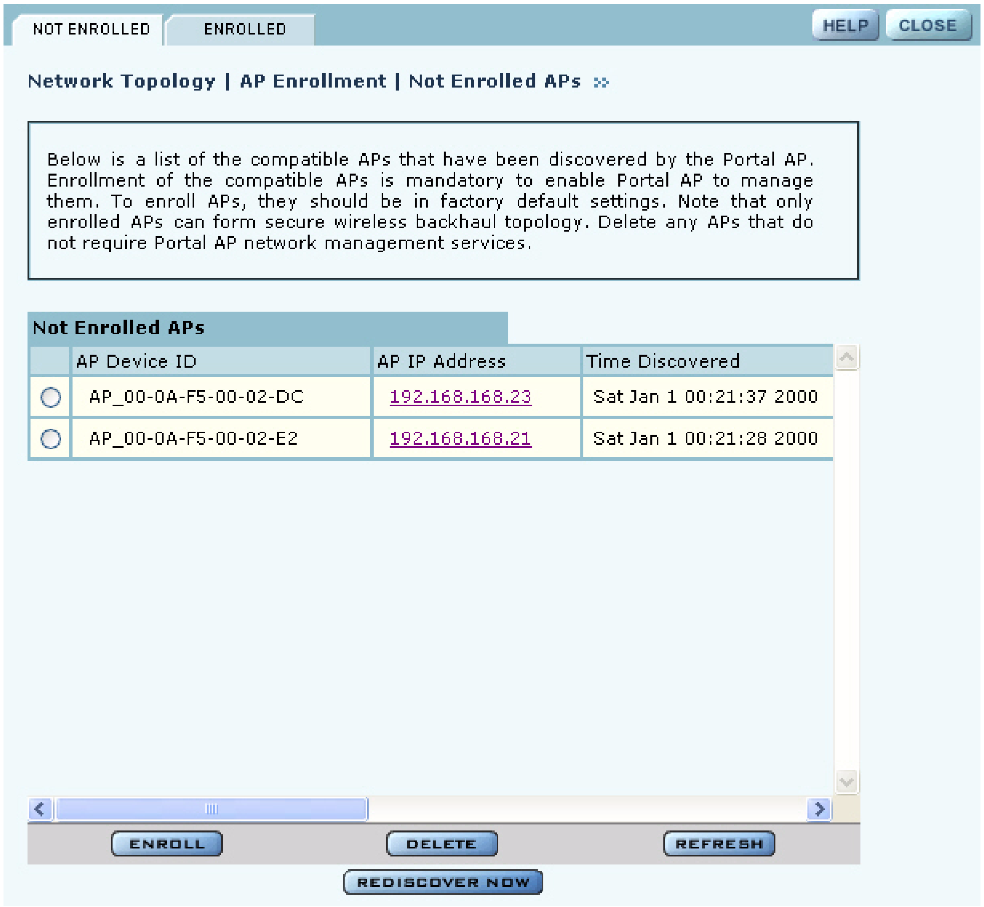


Figure 120: Network Topology - AP Enrollment - Not Enrolled



Network Topology | AP Enrollment | Not Enrolled APs

Below is a list of the compatible APs that have been discovered by the Portal AP. Enrollment of the compatible APs is mandatory to enable Portal AP to manage them. To enroll APs, they should be in factory default settings. Note that only enrolled APs can form secure wireless backhaul topology. Delete any APs that do not require Portal AP network management services.

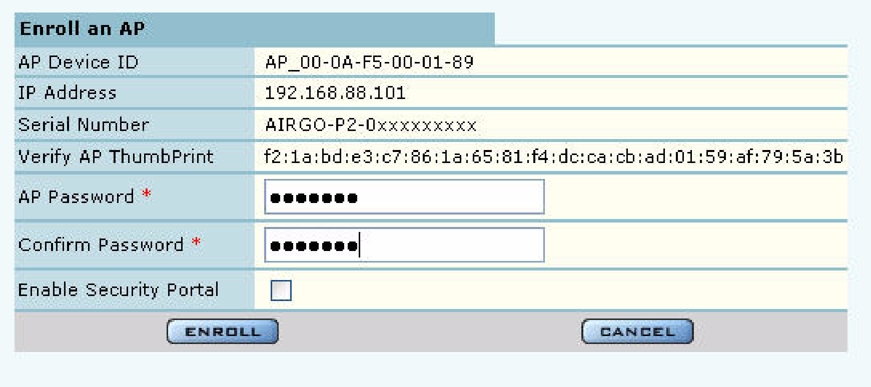
Not Enrolled APs

	AP Device ID	AP IP Address	Time Discovered
○	AP_00-0A-F5-00-02-DC	192.168.168.23	Sat Jan 1 00:21:37 2000
○	AP_00-0A-F5-00-02-E2	192.168.168.21	Sat Jan 1 00:21:28 2000

Perform the following functions from this panel:

Function	Description
Enroll an AP	**1** Select the desired AP, and click **Enroll** to open the Enroll an AP Entry panel (Figure 121). If the AP is not in the factory default state, a message is presented. Click the AP link to open the web interface for the AP and reset it to the factory default configuration. **2** After verifying the information on the panel (Table 13), enter the correct password, and click **Enroll**. It takes a couple of minutes to enroll the AP.
Delete an AP	Select an AP and click **Delete** to remove it from the list.
Refresh	Click to update the display.
Rediscover Now	Scan the network to discover APs and update the Not Enrolled APs table.

Figure 121: Network Topology - AP Enrollment - Enroll an AP Entry Panel



Enroll an AP

AP Device ID	AP_00-0A-F5-00-01-89
IP Address	192.168.88.101
Serial Number	AIRGO-P2-0xxxxxxxxx
Verify AP ThumbPrint	f2:1a:bd:e3:c7:86:1a:65:81:f4:dc:ca:cb:ad:01:59:af:79:5a:3b
AP Password *	•••••••
Confirm Password *	•••••••
Enable Security Portal	□

The Enroll an AP panel contains information that uniquely identifies the AP. To verify the identity of the AP, compare the following information to the information on the paperwork shipped with the AP:

Table 13: AP Enrollment Information

Field	Description
AP Name	Verify the alphanumeric name of the AP. The default is the IP address.
IP Address	Verify IP address of the AP.
Serial Number	Verify the AP serial number.
Thumbprint	Verify the thumbprint, which uniquely identifies the AP for security purposes.
Password	Enter and confirm the PLANEX-supplied password.
Security Portal	Indicate whether to use the AP as a standby security portal. With a backup security portal, a copy of the user authentication database remains accessible even if the NM Portal AP becomes unavailable.

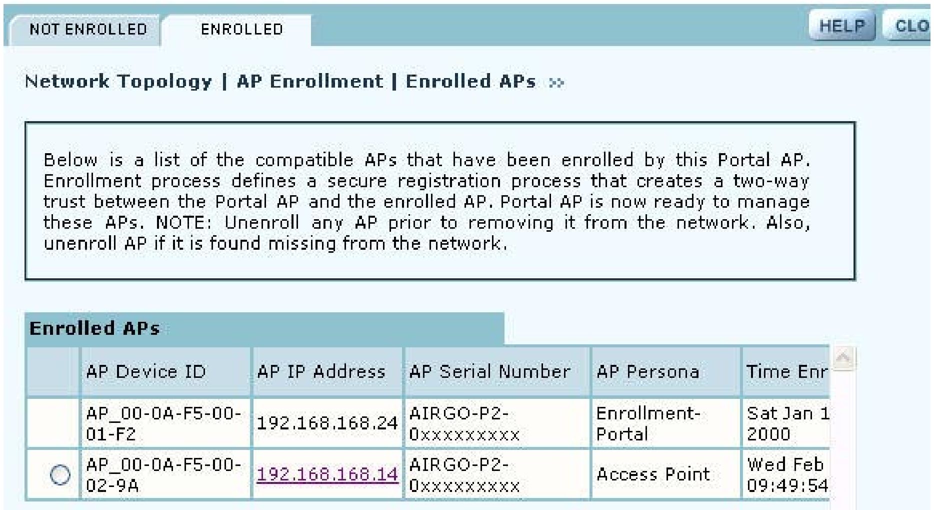
When an AP is enrolled, it is configured with the enrolling AP’s bootstrap configuration. Refer to Chapter 3, “Installing the Access Point,” for bootstrap configuration details.

Enrolled APs

Enrolled APs are listed on the Enrolled tab of the Enrollment panel (Figure 122). The screen should refresh automatically to reflect new enrollments. If this does not happen, click **Refresh**.

NOTE: If DHCP is used for address assignment for enrolled 108 Mbps Wireless APs, the AP address may change periodically. When that occurs, there is no interruption to service, and all security credentials remain intact.

Figure 122: Network Topology - AP Enrollment - Enrolled



Network Topology | AP Enrollment | Enrolled APs »

Below is a list of the compatible APs that have been enrolled by this Portal AP. Enrollment process defines a secure registration process that creates a two-way trust between the Portal AP and the enrolled AP. Portal AP is now ready to manage these APs. NOTE: Unenroll any AP prior to removing it from the network. Also, unenroll AP if it is found missing from the network.

Enrolled APs

	AP Device ID	AP IP Address	AP Serial Number	AP Persona	Time Enr
	AP_00-0A-F5-00-01-F2	192.168.168.24	AIRGO-P2-0xxxxxxxxx	Enrollment-Portal	Sat Jan 1 2000
○	AP_00-0A-F5-00-02-9A	192.168.168.14	AIRGO-P2-0xxxxxxxxx	Access Point	Wed Feb 09:49:54

Perform the following functions as needed from the Enrolled APs tab:

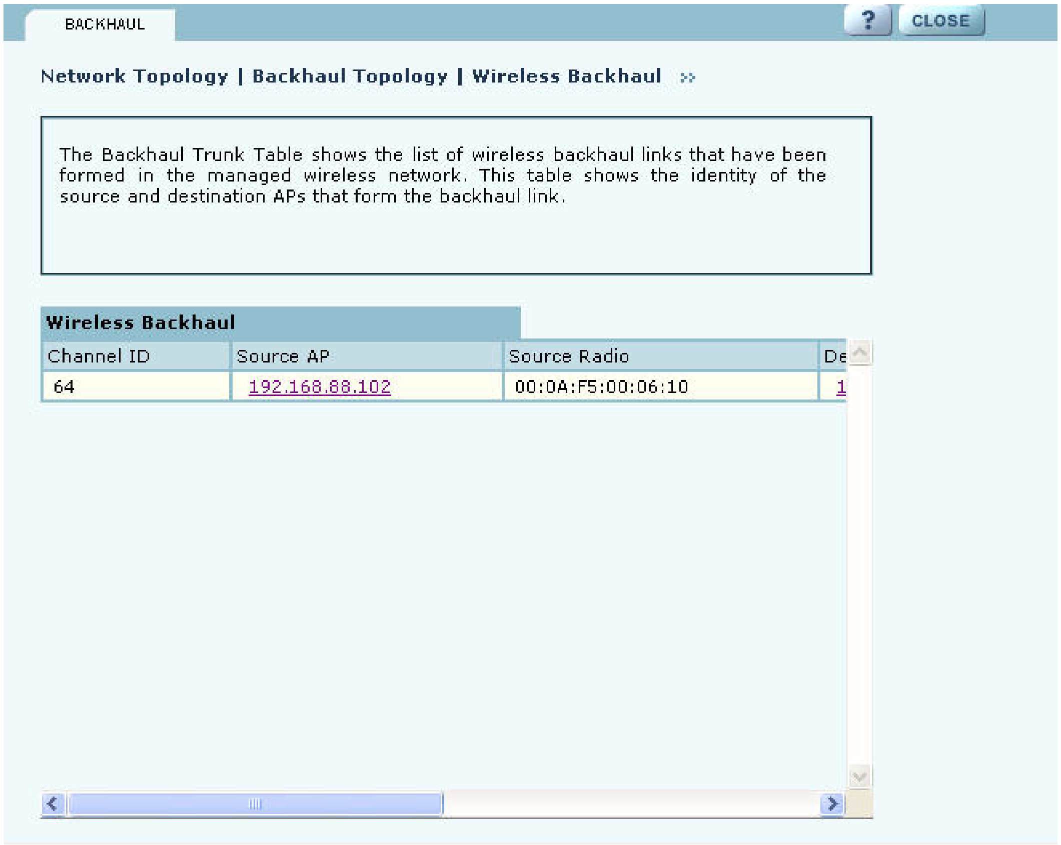
Function	Description
Unenroll	Remove the AP from the set of enrolled APs
Refresh	Update the screen display to reflect the most recent enrollment changes
Reboot	Reboot the selected AP
Click the IP address link for an AP	Access the web interface for the selected AP in a new browser window

NOTE: When an AP is unenrolled, the mutual trust between the NM Portal and the AP is destroyed and the unenrolled AP resets to factory defaults. The AP cannot be configured by NM Portal nor participate in the network (i.e., form a wireless backhaul) without being enrolled again.

Viewing Backhaul Topology

Configuring a wireless backhaul extends wireless network coverage while reducing the number of APs that must be connected to the wired network. Chapter 6, “Configuring a Wireless Backhaul,” explains how to configure the 108 Mbps Wireless AP to be part of a wireless backhaul. Once the wireless backhaul structure is in place, use the Backhaul Topology panel in NM Portal to view all the backhaul paths defined for the network. Choose **Backhaul Topology** from the Network Topology menu to display this information (Figure 123).

Figure 123: Network Topology - Backhaul Topology



The Backhaul Trunk Table shows the list of wireless backhaul links that have been formed in the managed wireless network. This table shows the identity of the source and destination APs that form the backhaul link.

Wireless Backhaul

Channel ID	Source AP	Source Radio	De
64	192.168.88.102	00:0A:F5:00:06:10	1

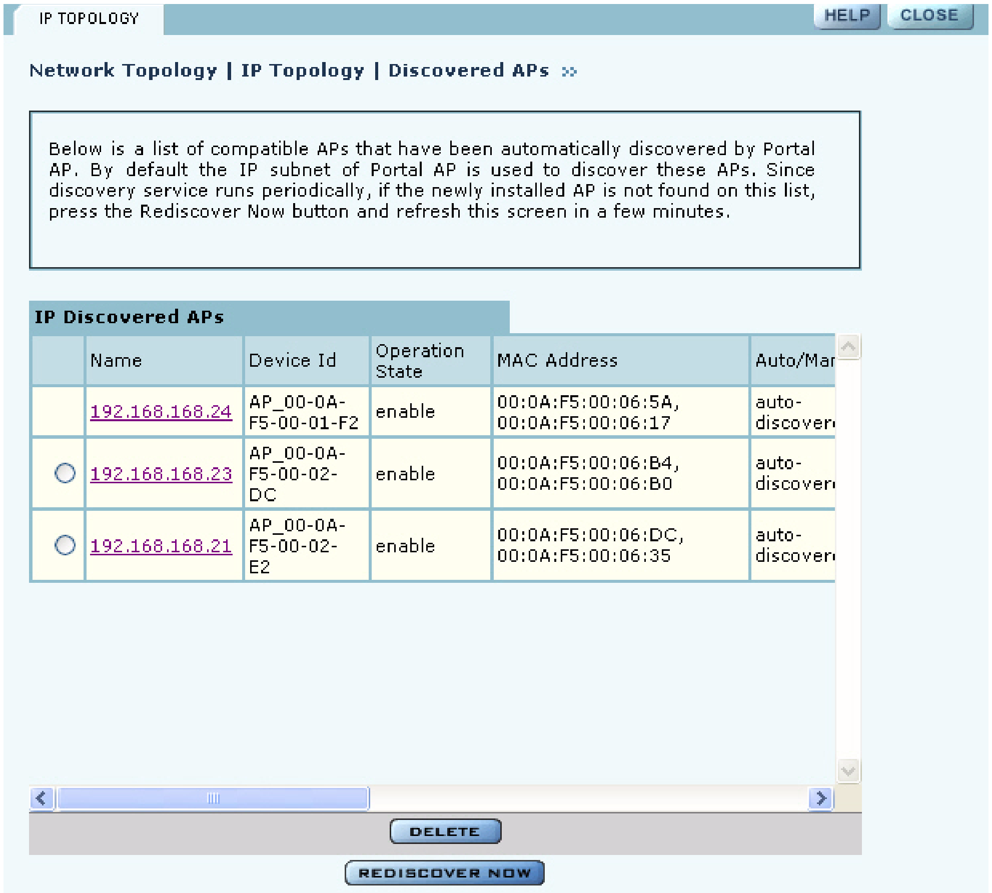
This panel contains the following information for each backhaul link:

Field	**Description**
Channel ID	RF channel over which the backhaul traffic travels
Source AP	AP that begins the uplink backhaul trunk. The Source AP link opens the web interface for the AP in a new browser window.
Source Radio	MAC address of the radio used for the uplink (wlan0 or wlan1).
Destination AP	MAC address of the radio that ends the backhaul trunk
Destination Radio	Radio used for the destination (wlan0 or wlan1)
Retrunk Count	The number of times a functioning backhaul radio reestablishes a trunk. A new backhaul can be established to any AP within RF range (retrunk does not necessarily mean re-connection to the same AP). If the retrunk count is high, the network has a high level of instability in its wireless inter-access point connections.
Rediscover Now button	Begins the rediscovery process.

Viewing IP Topology

The IP Topology panel lists all the APs discovered by NM Portal. Choose **IP Topology** from the Network Topology menu to display this information (Figure 124).

Figure 124: Network Topology - IP Topology



Network Topology | IP Topology | Discovered APs »

Below is a list of compatible APs that have been automatically discovered by Portal AP. By default the IP subnet of Portal AP is used to discover these APs. Since discovery service runs periodically, if the newly installed AP is not found on this list, press the Rediscover Now button and refresh this screen in a few minutes.

IP Discovered APs

	Name	Device Id	Operation State	MAC Address	Auto/Mar
	192.168.168.24	AP_00-0A-F5-00-01-F2	enable	00:0A:F5:00:06:5A, 00:0A:F5:00:06:17	auto-discover
○	192.168.168.23	AP_00-0A-F5-00-02-DC	enable	00:0A:F5:00:06:B4, 00:0A:F5:00:06:B0	auto-discover
○	192.168.168.21	AP_00-0A-F5-00-02-E2	enable	00:0A:F5:00:06:DC, 00:0A:F5:00:06:35	auto-discover

The table includes the following information for each AP:

Field	**Description**
Name	IP address assigned to the AP
Device ID	Unique AP identifier sent during the discovery process and required for AP enrollment. The device ID is included in the paperwork shipped with the AP.
Operation State	Indication of whether the AP can be reached from the NM Portal AP. The operation state is updated once every 5 minutes.
MAC Address	MAC addresses assigned to each of the AP radios. The address of the wlan0 radio is listed first and the wlan1 radio is listed second.
Auto/Manual	Indication of whether the AP was discovered automatically or manually identified

Field	Description
Portal Services	Indication of which portal services are configured on the AP (enrollment and security). Possible values: • Factory Default - AP has not yet been enrolled or bootstrapped. • Access Point - AP has been enrolled/bootstrapped as an AP • NM Portal- AP is enrolled/bootstrapped as NM Portal • SEC Portal - AP is enrolled/bootstrapped as a Security Portal • NM & SEC Portal - AP is enrolled/bootstrapped as NM Portal and Security Portal • Enrollment Portal - AP is bootstrapped as a Enrollment portal.
Time Discovered	Date and time of discovery
Enrollment State	Indication of whether the AP is enrolled (authorized) or not (unauthorized)
Thumbprint	Unique identifier used for security purposes. The thumbprint is included in the paperwork shipped with the AP.

View and check the status of all discovered APs from this panel. To delete an AP from the list, select the radio button to the left of the listing, and click **Delete**. Deleting an AP removes it from the topology database and deletes all the details about its configuration. However, since network discovery is a continuous process, it is possible for a deleted AP to be rediscovered if it is still part of the network.

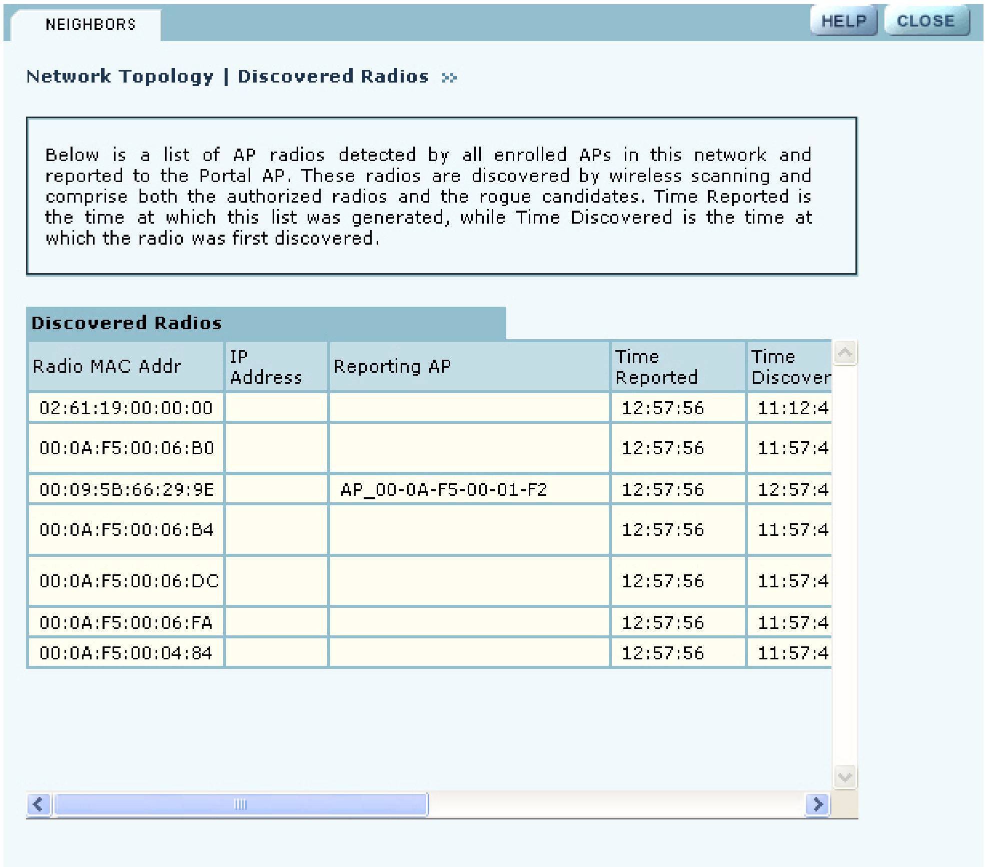
Use the delete feature when an AP is moved from one managed network to another.

Displaying Discovered Radios

Every 15 minutes, the NM Portal AP polls all the enrolled APs, which then report on all the wireless devices they can detect. The results of the polling are presented in the Discovered Radio table (Figure 125), accessible from the Discovered Radios item under Network Topology menu in the menu tree.

Use the Discovered Radios list to characterize the wireless network neighborhood and detect possible rogue APs.

Figure 125: Network Topology - Discovered Radios



Network Topology | Discovered Radios »

Below is a list of AP radios detected by all enrolled APs in this network and reported to the Portal AP. These radios are discovered by wireless scanning and comprise both the authorized radios and the rogue candidates. Time Reported is the time at which this list was generated, while Time Discovered is the time at which the radio was first discovered.

Discovered Radios

Radio MAC Addr	IP Address	Reporting AP	Time Reported	Time Discover
02:61:19:00:00:00			12:57:56	11:12:4
00:0A:F5:00:06:B0			12:57:56	11:57:4
00:09:5B:66:29:9E		AP_00-0A-F5-00-01-F2	12:57:56	12:57:4
00:0A:F5:00:06:B4			12:57:56	11:57:4
00:0A:F5:00:06:DC			12:57:56	11:57:4
00:0A:F5:00:06:FA			12:57:56	11:57:4
00:0A:F5:00:04:84			12:57:56	11:57:4

The Discovered Radios table contains the following information for each detected device:

Field	Description
MAC Address	Address that uniquely identifies the detected device
IP Address	IP address of the detected device, if known
Reporting AP	The enrolled AP which reported the device to the NM Portal AP. If this field is blank, the AP was reported on a previous scan, but not the most recent one.
Time Reported	The time of the last scan that detected the AP
Time Discovered	The time of day that the presence of the device was discovered by the reporting AP
Class	Indication of whether the discovered node is just a Radio Neighbor or a Radio and IP Neighbor. Radio and IP neighbors are part of the internal network (they are reachable by way of IP addressing).
Signal Strength	Strength of the detected signal as a percentage
SSID	The SSID of the detected device, if known
Channel ID	The channel on which the signal was detected
BSS Type	Whether the detected device is part of an infrastructure or ad-hoc service set

Managing Rogue Access Points

A rogue AP is an access point that connects to the wireless network without authorization. In some cases, the AP may be performing a legitimate function and the appropriate management action is to classify the AP as “known.” If it is not possible to identify a legitimate role for the AP, then the AP is considered to be a true rogue. NM Portal provides information to help determine where rogue APs are physically located and how recently they have accessed the network. With this information, it may be possible to find and disable them.

NOTE: Use the Discovery Configuration panel to enable the rogue AP discovery feature. For instructions, see “Configuring Network Discovery” on page 184.

Potential rogue AP candidates are identified during discovery. Every 15 minutes NM Portal scans the network to discover and identify known 108 Mbps Wireless APs. The domain for the discovery process is specified in the Discover Configuration panel (see “Configuring Network Discovery” on page 184). Discovery can be restricted to specific subnetworks, ranges of IP addresses, or individual APs. It is also possible to specify whether the discovery is at the IP (layer 3) or wireless/ MAC level (layer 2).

Wireless discovery is based on the beacon sent by APs within range of the receiving AP. Each AP collects information about beacons it sees and passes that information to NM Portal. NM Portal checks the MAC address of the detected AP to see whether it matches that of a known AP. If it does not match, the detected AP becomes a rogue AP candidate.

IP level discovery requires that the detecting AP be able to determine the IP address of the discovered AP through an IP / SNMP connectivity check and establish IP level communications with it. NM Portal then performs a series of consistency checks and certification to determine whether the AP is a recognized part of the network.

After an AP is successfully discovered and authenticated, the system checks to see whether it is enrolled and places it into the Enrolled or APs to be Enrolled table. For more information on AP enrollment, see “Enrolling APs” on page 167.A variety of conditions may cause NM Portal to label an AP as a rogue candidate:

- The AP is in a subnet not included in the discovery domain.
- The AP is not an 108 Mbps Wireless AP.
- A problem exists with the AP certificate, and the AP cannot be authenticated.
- The AP is a legitimate device on a neighboring network, but has been detected through a wireless scan.
- An unauthorized device attempts to access the network

The objectives of rogue AP management are to determine which APs pose a security risk and to take action to reduce the risk.

The Rogue AP panels within NM Portal provide an interface to monitor and classify rogue APs. Use the IP Rogue AP panel to manage potential rogues detected through IP discovery, and use the Wireless Rogue AP panel to manage potential rogues detected through wireless discovery.

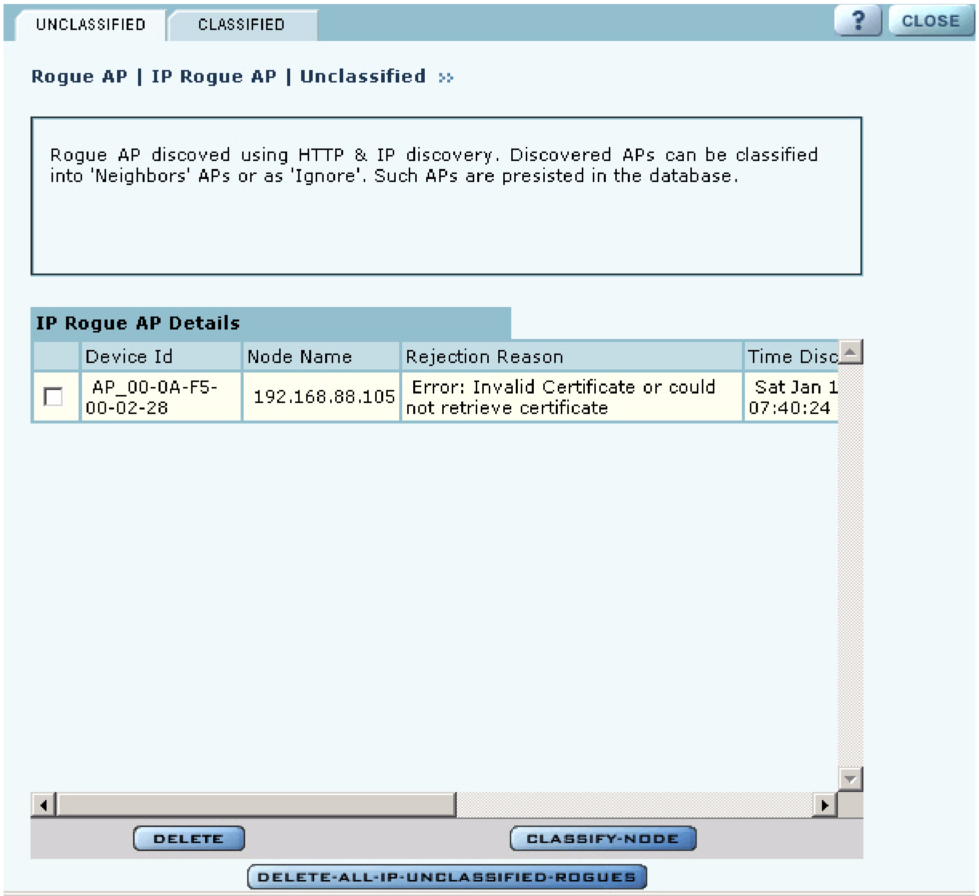
Each panel opens to the Unclassified tab, which lists the candidate rogue APs. From the list, select individual APs to classify as known in your network or a neighbor’s network. Once classified, the APs are listed in the IP or Wireless Classified tab.

IP Rogue AP Management

Select IP Rogue AP from the Rogue AP menu to open the table of IP-unclassified APs. This panel (Figure 126) lists the following information for each unclassified AP:

Field	Description
Device ID	Unique identifier for the AP
Node Name	Name of the AP advertised in the beacon frame
Rejection Reason	Failure that prevented the AP from passing authentication
Time Discovered	Time of the last IP scan that detected the AP. This value is updated each time the AP is detected.
Thumbprint	Factory-generated identifier used for AP enrollment

Figure 126: IP Rogue AP - Unclassified



Rogue AP | IP Rogue AP | Unclassified »

Rogue AP discoved using HTTP & IP discovery. Discovered APs can be classified into 'Neighbors' APs or as 'Ignore'. Such APs are presisted in the database.

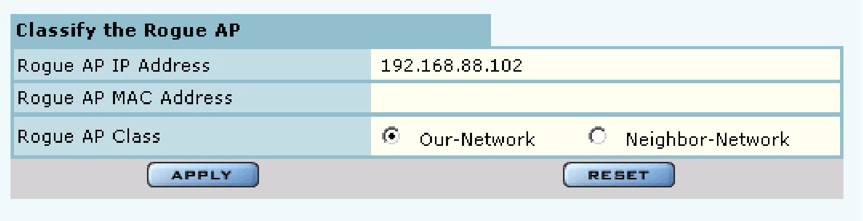
IP Rogue AP Details

	Device Id	Node Name	Rejection Reason	Time Disc
□	AP_00-0A-F5-00-02-28	192.168.88.105	Error: Invalid Certificate or could not retrieve certificate	Sat Jan 1 07:40:24

Perform the following functions from this tab:

Function	Steps
Classify an AP as known	1 Select the AP from the list. APs are identified by PLANEX device ID and IP address, if known. 2 Click **Classify-Node** to open the Classify the Rogue AP panel (Figure 127). 3 Select **Our-Network** to classify the AP as known within your wireless network. Select **Neighbor-Network** to classify the AP as known in a neighboring network. 4 Click **Apply**. The AP is now classified. The classification information is retained in the NM Portal database and presented on the Classified tab (Figure 128). This information is retained upon AP reboot.
Delete an AP from the rogue list	Click **Delete** and click **OK** to confirm. If an AP is deleted from the list and then discovered in a subsequent scan, it is added to the list again.
Delete from the list all APs classified as IP rogues	Click **Delete all IP-Unclassified Rogues**, and click **OK** to confirm.

Figure 127: IP Rogue AP - Classify



Classify the Rogue AP

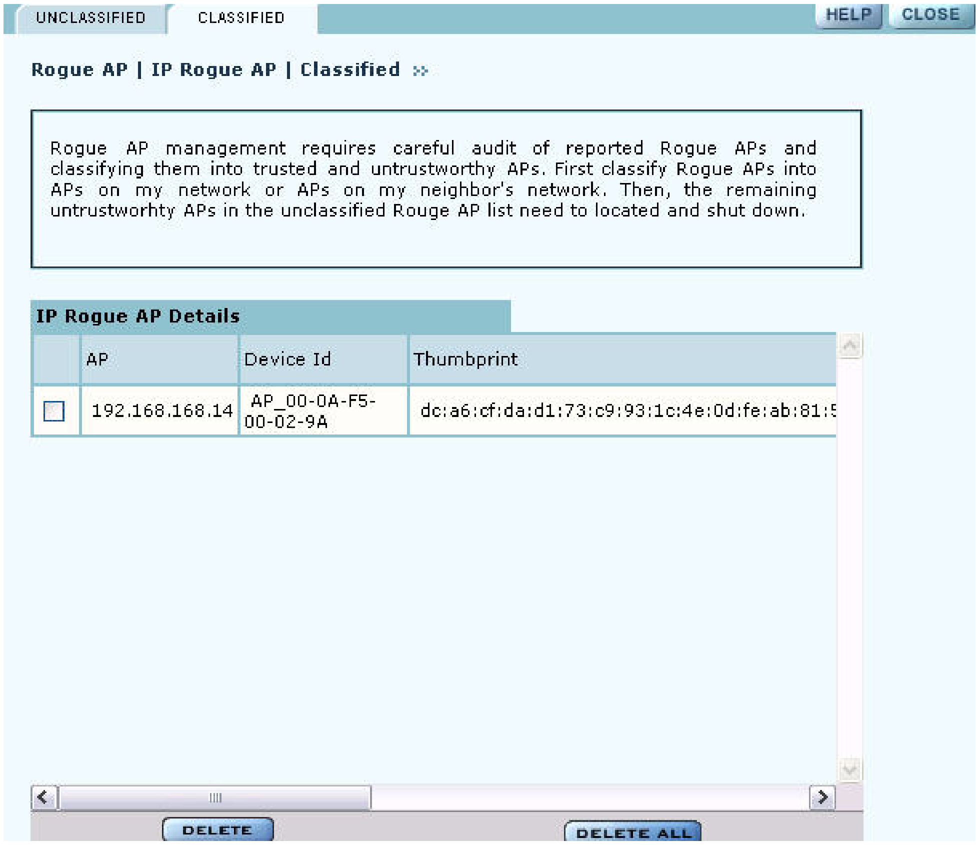
Rogue AP IP Address	192.168.88.102
Rogue AP MAC Address	
Rogue AP Class	● Our-Network ○ Neighbor-Network

Classified Tab

The Classified tab (Figure 128) lists all the APs designated as known through IP classification. It contains the following information for each classified AP:

Field	Description
AP	Name of the AP, by default, the MAC address
Device ID	Unique identifier for the AP
Thumbprint	Factory-generated identifier used for AP enrollment
Portal Services	Portal services (enrollment, security, NM portal) configured on the AP
Operational State	Indicator of whether the AP is currently active
Discovery Method	IP or wireless discovery
Time Discovered	Time of the last IP scan that detected the AP. This value is updated each time the AP is detected.
Node State	Identifies whether the AP has been classified as a member of Our-Network or Neighbor-Network
MAC Address	MAC address of the AP

Figure 128: IP Rogue AP - Classified



Rogue AP | IP Rogue AP | Classified

Rogue AP management requires careful audit of reported Rogue APs and classifying them into trusted and untrustworthy APs. First classify Rogue APs into APs on my network or APs on my neighbor's network. Then, the remaining untrustworhty APs in the unclassified Rouge AP list need to located and shut down.

IP Rogue AP Details

	AP	Device Id	Thumbprint
□	192.168.168.14	AP_00-0A-F5-00-02-9A	dc:a6:cf:da:d1:73:c9:93:1c:4e:0d:fe:ab:81:!

Wireless Rogue AP Management

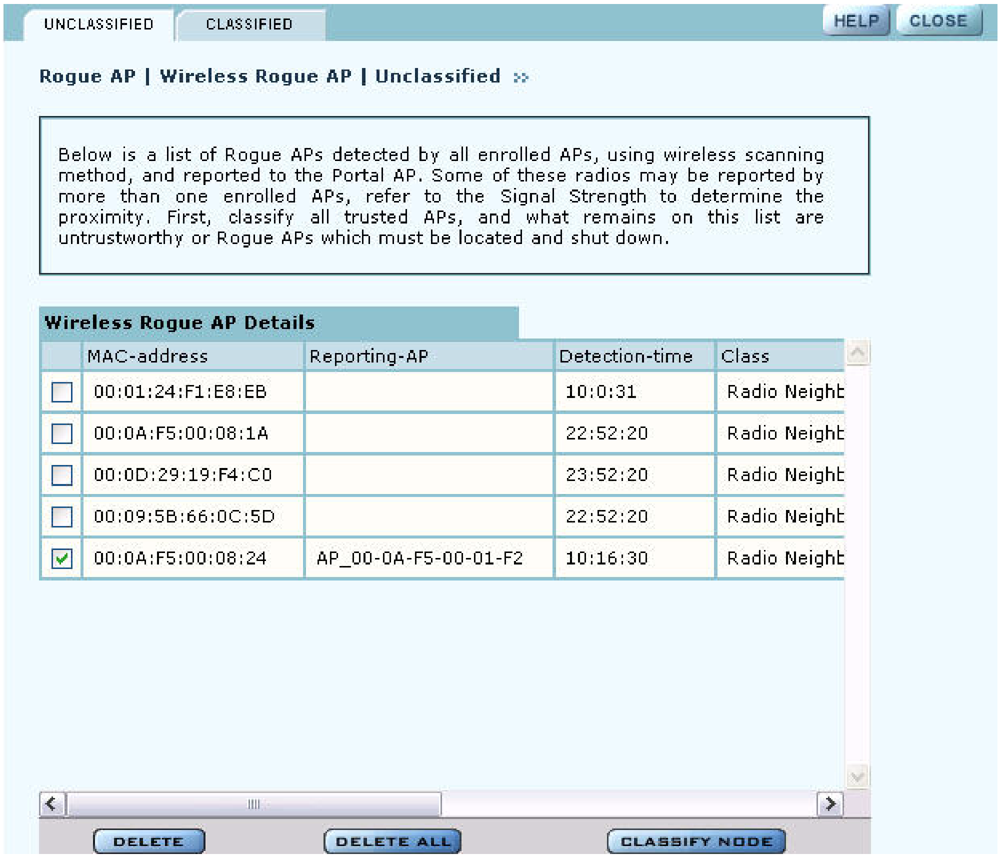
Wireless rogue management differs from IP rogue management in the type of discovery used to determine whether the AP is authorized to be part of the network. In wireless discovery, each AP scans the beacons sent by other APs within range and attempts to identify the APs from the information in the beacon.

Select Wireless Rogue AP from the Rogue AP menu to open the table of unclassified wireless rogue APs. This panel (Figure 129) lists the following information for each IP rogue:

Field	Description
MAC Address	MAC address of the unclassified rogue AP
Reporting AP	The device ID of the AP or APs that identified the rogue AP. If this field is empty, that means that the rogue device was detected in a previous scan, but not in the most recent scan.
Detection Time	Time that the AP was last detected
Class	Radio Neighbor or Radio & IP Neighbor
Signal Strength	Strength of the beacon (dBm)
BSS Type	Infrastructure or ad-hoc (IBSS)
SSID	SSID sent in the rogue beacon
Channel ID	Radio channel on which the AP was discovered

Field	Description
Reporting Time	Time of the last wireless scan

Figure 129: Wireless Rogue AP - Unclassified



Rogue AP | Wireless Rogue AP | Unclassified »

Below is a list of Rogue APs detected by all enrolled APs, using wireless scanning method, and reported to the Portal AP. Some of these radios may be reported by more than one enrolled APs, refer to the Signal Strength to determine the proximity. First, classify all trusted APs, and what remains on this list are untrustworthy or Rogue APs which must be located and shut down.

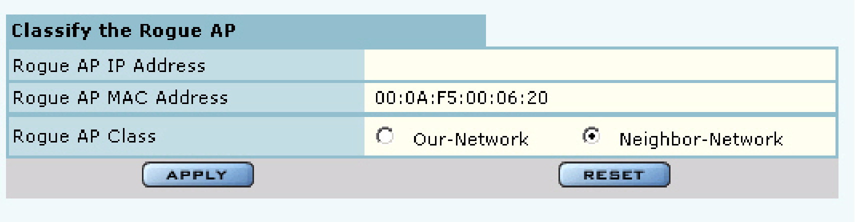
Wireless Rogue AP Details

	MAC-address	Reporting-AP	Detection-time	Class
□	00:01:24:F1:E8:EB		10:0:31	Radio Neighb
□	00:0A:F5:00:08:1A		22:52:20	Radio Neighb
□	00:0D:29:19:F4:C0		23:52:20	Radio Neighb
□	00:09:5B:66:0C:5D		22:52:20	Radio Neighb
☑	00:0A:F5:00:08:24	AP_00-0A-F5-00-01-F2	10:16:30	Radio Neighb

Perform the following functions from this tab:

Function	Steps
Classify an AP as known	1 Select the AP from the list. APs are identified by MAC address. 2 Click **Classify-Node** to open the Classify the Rogue AP panel (Figure 130). 3 Select **Our-Network** to classify the AP as known within your wireless network. Select **Neighbor-Network** to classify the AP as known in a neighboring network. 4 Click **Apply**. The AP is now classified. The classification information is retained in the NM Portal database and presented on the Classified tab (Figure 131). This information is retained upon AP reboot.
Delete an AP from the rogue list	Click **Delete** and click **OK** to confirm. If an AP is deleted from the list and then discovered in a subsequent scan, it is added to the list again.
Delete from the list all APs classified as wireless rogues	Click **Delete All**, and click **OK** to confirm

Figure 130: Wireless Rogue AP - Classify



Classify the Rogue AP

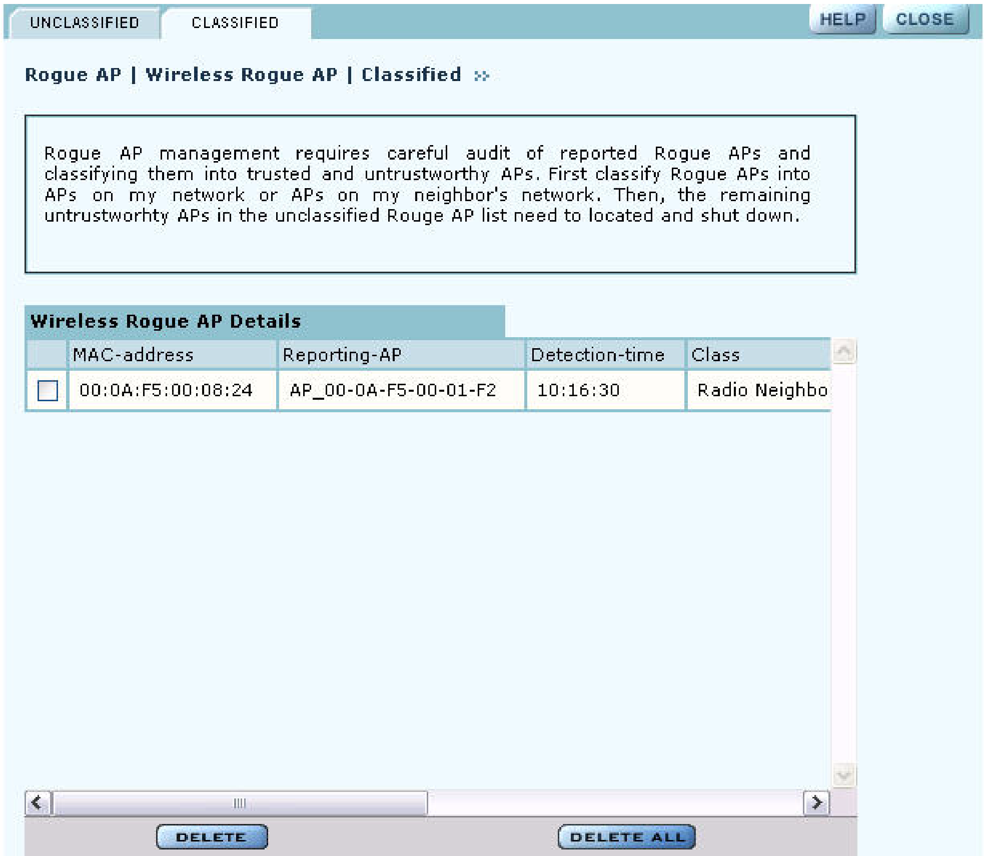
Rogue AP IP Address	
Rogue AP MAC Address	00:0A:F5:00:06:20
Rogue AP Class	○ Our-Network ● Neighbor-Network

Classified Tab

The Classified tab (Figure 131) lists all the APs designated as known through wireless classification. It contains the following information for each AP:

Field	Description
MAC Address	Name of the detected AP, by default, the MAC address
Reporting AP	IP address of the AP that reported the detected AP
Detection Time	Time of the scan that last detected the AP
Class	Category used to classify the AP

Figure 131: Wireless Rogue AP - Classified



Rogue AP | Wireless Rogue AP | Classified »

Rogue AP management requires careful audit of reported Rogue APs and classifying them into trusted and untrustworthy APs. First classify Rogue APs into APs on my network or APs on my neighbor's network. Then, the remaining untrustworhty APs in the unclassified Rouge AP list need to located and shut down.

Wireless Rogue AP Details

	MAC-address	Reporting-AP	Detection-time	Class
□	00:0A:F5:00:08:24	AP_00-0A-F5-00-01-F2	10:16:30	Radio Neighbo

Using the NM Services Menu

Use the NM Services menu to define and manage policies, configure parameters for network discovery, add information about DHCP servers, and add portals at remote locations.

Working With Policies

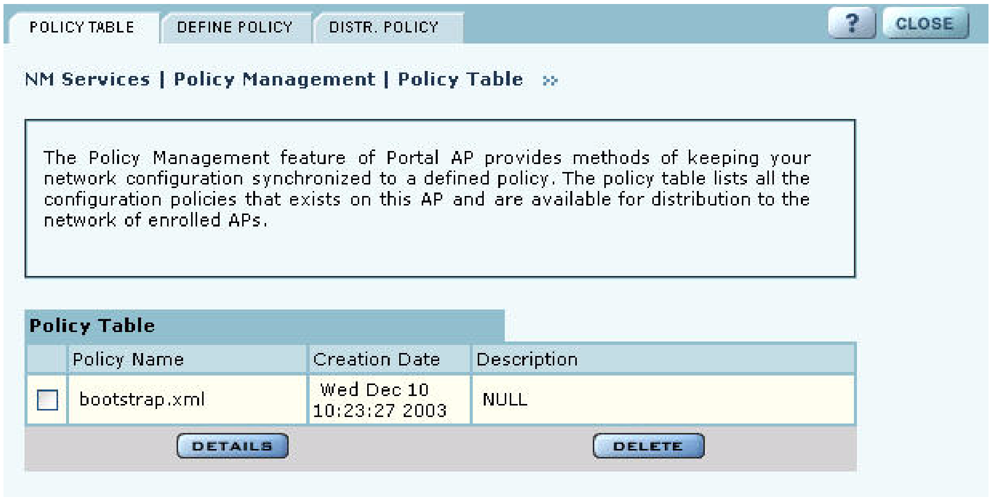
Policy Management provides tools to keep your network configuration synchronized to a defined set of rules. Open the Policy Management panel to manage configuration policies for distribution to the network of enrolled APs. The panel contains the following tabs:

- Policy Table—View existing policies.
- Define Policy—Specify a policy for bootstrapping other APs in the network.
- Distribute Policy—Send a policy to other APs in the network.

Policy Table

The policy table (Figure 132) lists policies that exist on this AP and are available for distribution to the network of enrolled APs.

Figure 132: NM Services - Policy Management - Policy Table



NM Services | Policy Management | Policy Table »

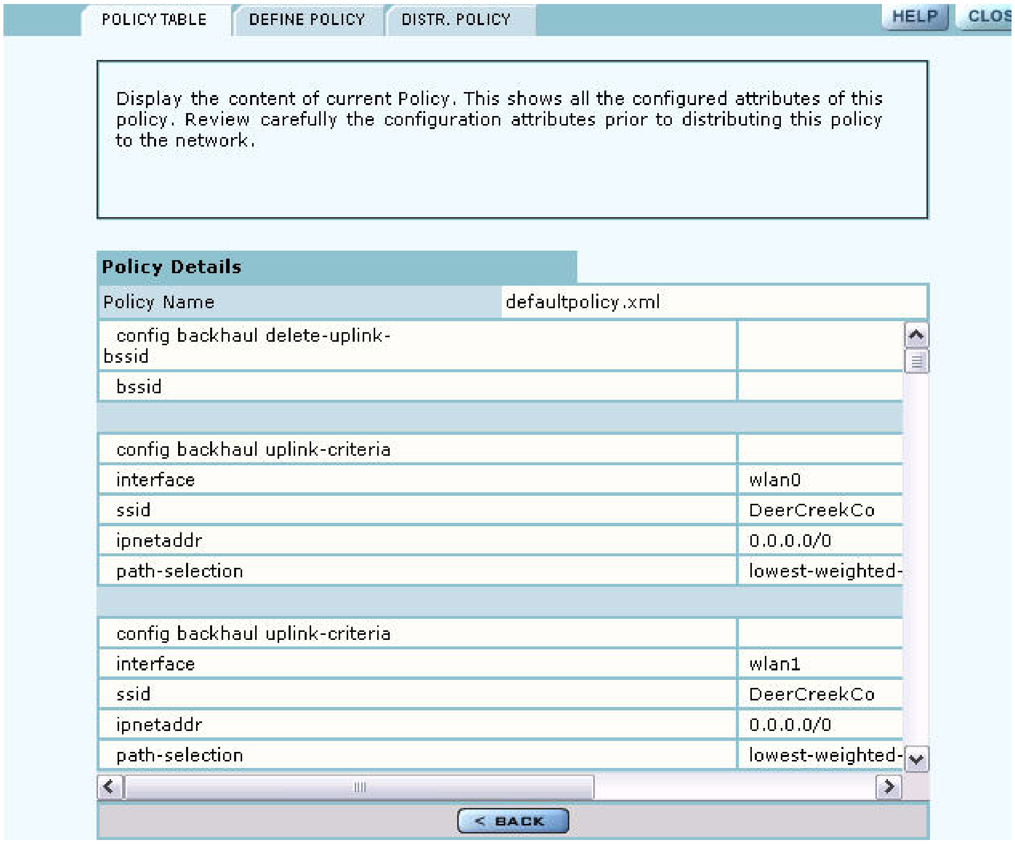
The Policy Management feature of Portal AP provides methods of keeping your network configuration synchronized to a defined policy. The policy table lists all the configuration policies that exists on this AP and are available for distribution to the network of enrolled APs.

Policy Table

	Policy Name	Creation Date	Description
□	bootstrap.xml	Wed Dec 10 10:23:27 2003	NULL

To view the details of a policy, select the name in the policy table, and click **Details**. The policy table expands to display all the parameters contained in the policy (Figure 132). To return to the policy table, click **Back**. To delete a policy, click **Delete**.

Figure 133: NM Services - Policy Management - Policy Table - Details (excerpt)



Display the content of current Policy. This shows all the configured attributes of this policy. Review carefully the configuration attributes prior to distributing this policy to the network.

Policy Details

Policy Name	defaultpolicy.xml
config backhaul delete-uplink-bssid	
bssid	
config backhaul uplink-criteria	
interface	wlan0
ssid	DeerCreekCo
ipnetaddr	0.0.0.0/0
path-selection	lowest-weighted-
config backhaul uplink-criteria	
interface	wlan1
ssid	DeerCreekCo
ipnetaddr	0.0.0.0/0
path-selection	lowest-weighted-

Define Policy

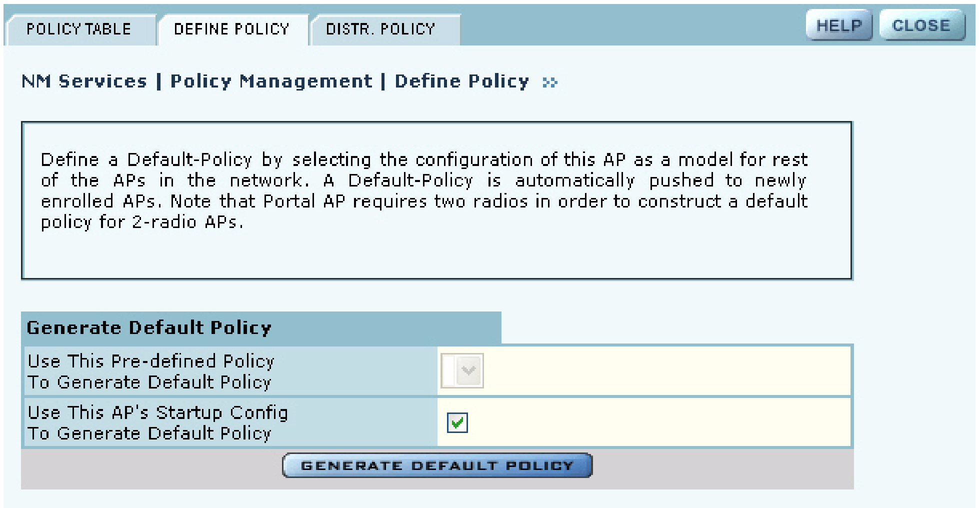
Define a default policy for bootstrapping other APs in the network by selecting the configuration of this AP as a model. The default policy is pushed automatically to newly enrolled APs. Use the Define Policy tab (Figure 134) to choose the default policy.

NOTE: The Portal AP requires two radios in order to construct a default policy for 2-radio APs.

Perform the following functions from this tab:

Function	Description
Generate a default policy from a pre-defined policy	Select a policy from the pull-down list, and click **Apply**. Not currently supported.
Use this AP’s start-up configuration to generate a default policy.	Select the checkbox, and click **Apply**.

Figure 134: NM Services - Policy Management - Define Policy



NM Services | Policy Management | Define Policy »

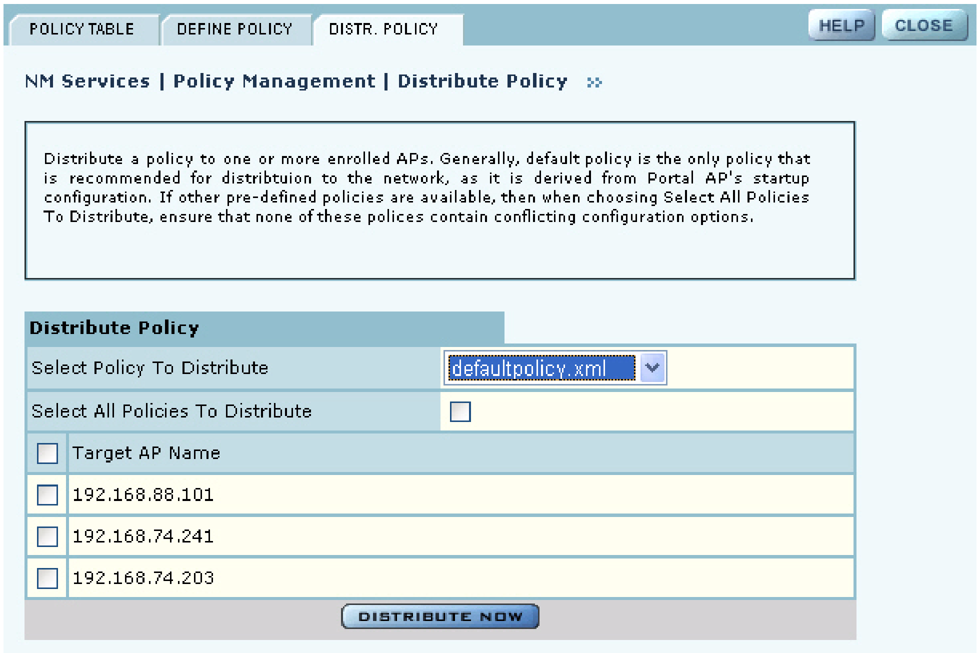
Define a Default-Policy by selecting the configuration of this AP as a model for rest of the APs in the network. A Default-Policy is automatically pushed to newly enrolled APs. Note that Portal AP requires two radios in order to construct a default policy for 2-radio APs.

Generate Default Policy	
Use This Pre-defined Policy To Generate Default Policy	
Use This AP's Startup Config To Generate Default Policy	☑

Distribute Policy

Use the Distribute Policy tab (Figure 135) to direct how policies are shared across the network.

Figure 135: NM Services - Policy Management - Distribute Policy



NM Services | Policy Management | Distribute Policy »

Distribute a policy to one or more enrolled APs. Generally, default policy is the only policy that is recommended for distribtuion to the network, as it is derived from Portal AP's startup configuration. If other pre-defined policies are available, then when choosing Select All Policies To Distribute, ensure that none of these polices contain conflicting configuration options.

Distribute Policy	
Select Policy To Distribute	defaultpolicy.xml
Select All Policies To Distribute	□

□	Target AP Name
□	192.168.88.101
□	192.168.74.241
□	192.168.74.203

Configure the following fields on this tab:

Field	Description
Select Policy to Distribute	Select an existing policy from the pull-down list.
Select All Policies to Distribute	Select to distribute all the existing policies.

Field	Description
Target AP Name	Select the APs to receive the policy or policies, or select **Target AP Name** to distribute to all the APs.

Click **Distribute Now** to send the policies to the designated APs.

Configuring Network Discovery

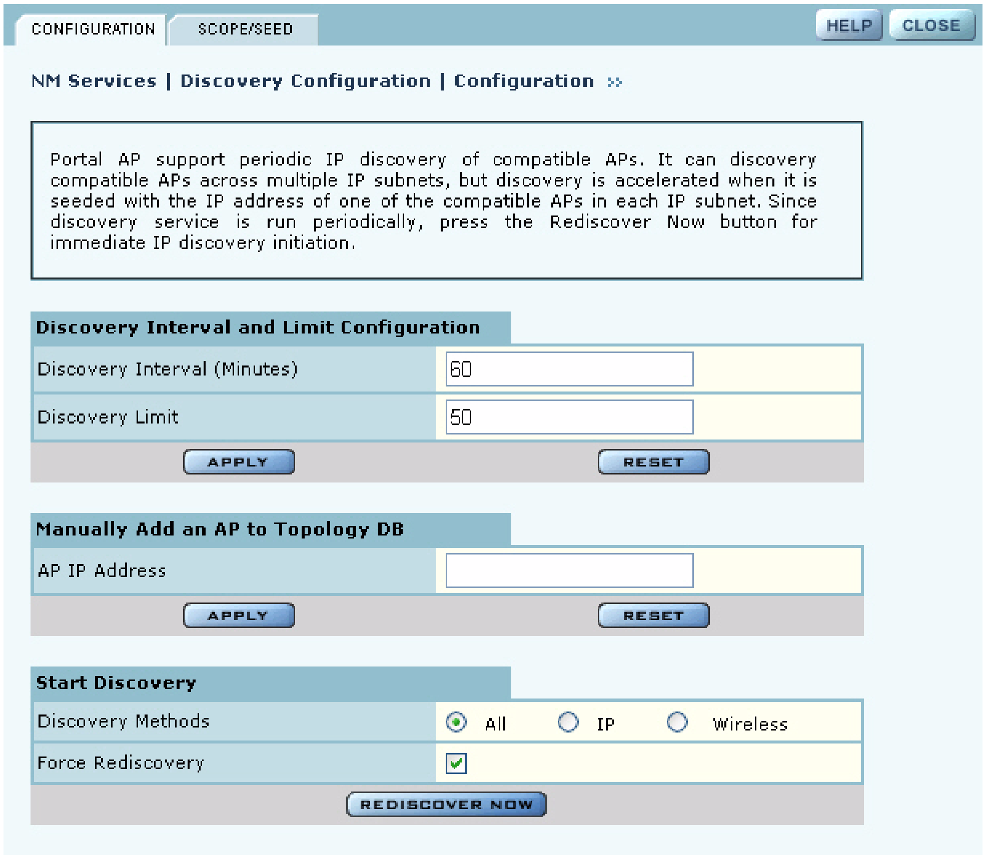
Use the Network Discovery panel to set up the rules for AP discovery.The panel contains the following tabs:

- Configuration—Specify discovery parameters.
- Scope/Seed—Restrict discovery to specified subnetworks or IP address ranges.
- Rogue AP—Enable or disable rogue AP discovery.

Configuration

Select Network Discovery from the NM Services menu to open the Configuration panel (Figure 136).

Figure 136: NM Services - Discovery Configuration



NM Services | Discovery Configuration | Configuration »

Portal AP support periodic IP discovery of compatible APs. It can discovery compatible APs across multiple IP subnets, but discovery is accelerated when it is seeded with the IP address of one of the compatible APs in each IP subnet. Since discovery service is run periodically, press the Rediscover Now button for immediate IP discovery initiation.

Discovery Interval and Limit Configuration	
Discovery Interval (Minutes)	60
Discovery Limit	50

Manually Add an AP to Topology DB	
AP IP Address	

Start Discovery	
Discovery Methods	● All ○ IP ○ Wireless
Force Rediscovery	☑

Configure the following values on this tab:

Field	Description
Discovery Interval	Restrict discovery to a time interval (in minutes). The range is 60-10080 (default is 60).

Field	Description
Discovery Limit	Restrict discovery to a number of APs. Once this limit is reached, the discover process stops. The range is 1-50 for (default is 50 APs).
AP IP Address	Specify the IP address of an AP that you want to manage but which is not part of the managed subnetwork specified in the discovery scope. AP's added to the managed network this way are termed “manually added” and can be managed by NM Portal. This option is useful if an AP is moved to another subnet and is no longer able to reach the NM Portal AP. You can manually add the AP’s IP address in NM Portal and continue manage the AP. It is not necessary to reenroll the AP.
Discovery Methods	Select whether to discover the APs with valid IP address information (IP), those identifiable by their radio beacon (Wireless), or those that meet either criterion.
Force Rediscovery	Select to force an immediate rediscovery of all APs. If the discovery process is already in progress when rediscovery is initiated, then no additional discovery is re-initiated. To stop the current discovery process and restart discovery again, use the Force All option. This is useful if the discovery scope is incorrectly configured and must be deleted.

Click **Apply** to implement the changes in each section or **Reset** to return to previously saved values.

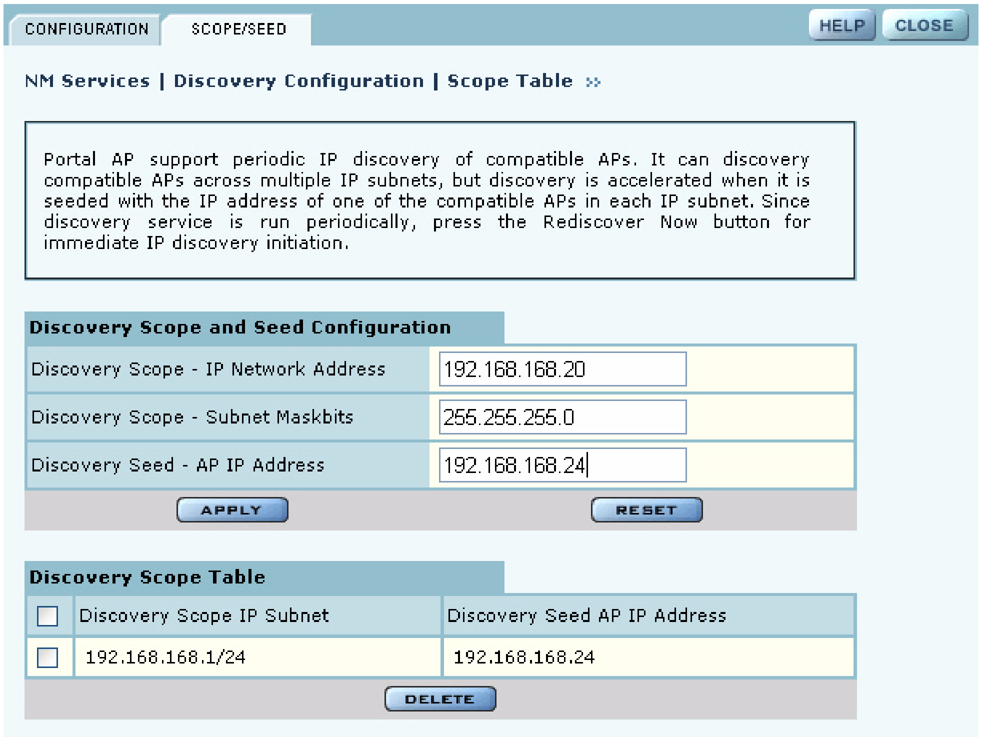
Use the Start Discovery radio buttons at the bottom of the panel to configure discovery on demand. Choices are to discover all APs, only those with a connection to the wired network (IP), or only those that radio neighbors. Click **Discover** to rediscover the network on demand.

Scope/Seed

By default, NM Portal automatically discovers all compatible APs in the local IP subnet. When APs are deployed across multiple subnetworks, specifying the discovery scope and seed IP address speeds the discovery process. The seed IP address is used as the reference AP for discovery purposes. The Seed AP is optional. If it is not specified, NM Portal automatically discovers all the compatible APs in that subnet and identifies a seed AP for itself.

Select the Scope/Seed tab (Figure 136) to configure the scope and seed parameters.

Figure 137: NM Services - Discovery Configuration - Scope/Seed



NM Services | Discovery Configuration | Scope Table »

Portal AP support periodic IP discovery of compatible APs. It can discovery compatible APs across multiple IP subnets, but discovery is accelerated when it is seeded with the IP address of one of the compatible APs in each IP subnet. Since discovery service is run periodically, press the Rediscover Now button for immediate IP discovery initiation.

Discovery Scope and Seed Configuration

Discovery Scope - IP Network Address	192.168.168.20
Discovery Scope - Subnet Maskbits	255.255.255.0
Discovery Seed - AP IP Address	192.168.168.24

Discovery Scope Table

□	Discovery Scope IP Subnet	Discovery Seed AP IP Address
□	192.168.168.1/24	192.168.168.24

Configure the following fields on this tab:

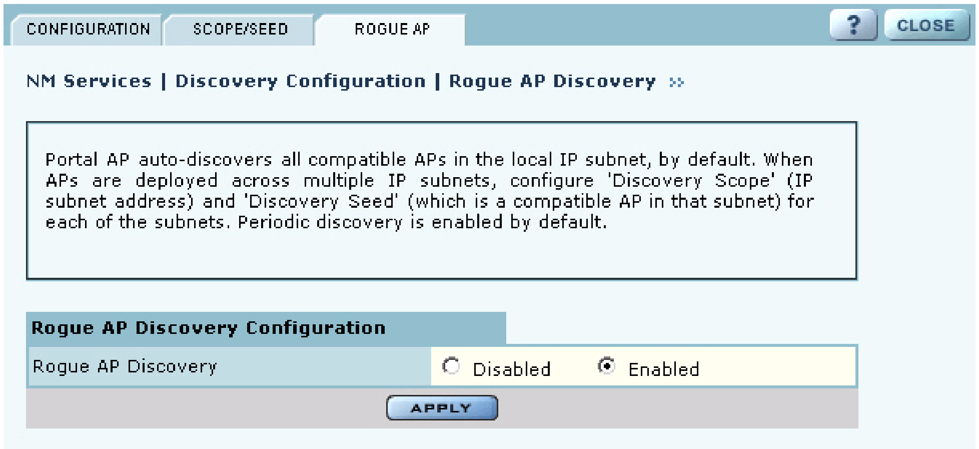
Field	**Description**
Discovery Scope	Enter the IP address of the subnet that you want to discover.
Discovery Scope - Subnet Maskbits	Enter the subnet prefix length for the discovery scope.
Discovery Seed	Specify a seed IP, which is the first address NM Portal will attempt to discover in the selected subnetwork.

Click **Apply** to save the selections and add them to the Discovery Scope Table at the bottom of the panel.

Rogue AP

Use the Rogue AP tab (Figure 136) to enable or disable discovery of rogue access points. The default is Enabled. Click **Apply** to save the setting. If enabled, NM Portal automatically scans the network to detect IP and wireless rogue access points. For more information, see “Managing Rogue Access Points” on page 175.

Figure 138: NM Services - Discovery Configuration - Rogue AP


CONFIGURATION
SCOPE/SEED
ROGUE AP
?
CLOSE
NM Services | Discovery Configuration | Rogue AP Discovery »
APPLY

Portal AP auto-discovers all compatible APs in the local IP subnet, by default. When APs are deployed across multiple IP subnets, configure 'Discovery Scope' (IP subnet address) and 'Discovery Seed' (which is a compatible AP in that subnet) for each of the subnets. Periodic discovery is enabled by default.

Rogue AP Discovery Configuration	
Rogue AP Discovery	○ Disabled ● Enabled

Configuring Portals

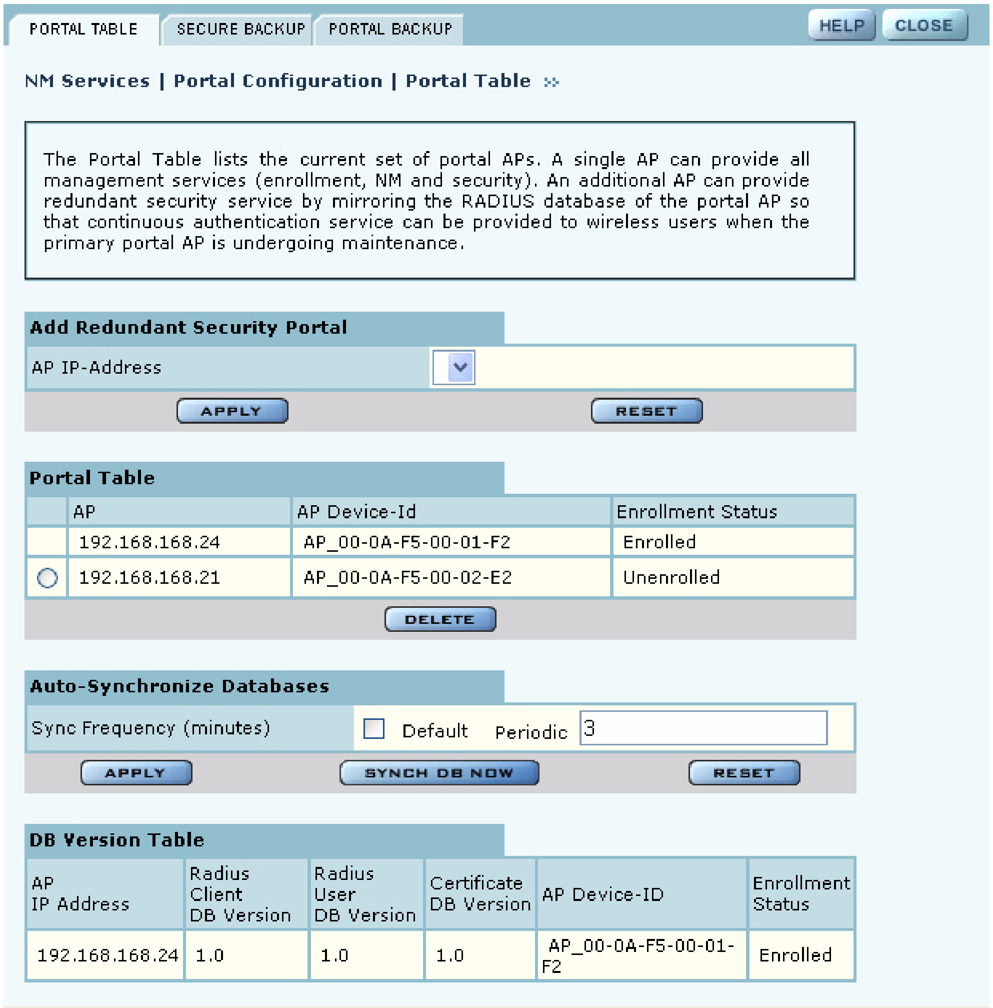
The Portal Configuration panel lists all the 108 Mbps Wireless Access Point portals that your AP has discovered and permits addition of a standby security portal to ensure that the wireless user authentication service remains available even if the NM Portal AP temporarily loses its connection. The panel contains two tabs:

- Portal Table—Add a redundant security portal and synchronize the portal databases.
- Secure Backup—Use https to perform a secure backup of the NM Portal AP configuration.
- Portal Backup—Back up or restore the portal databases and configuration.

Portal Table

Use the Portal Table (Figure 139) to manage the security portals for the network.

Figure 139: NM Services - Portal Configuration - Portal Table



NM Services | Portal Configuration | Portal Table »

The Portal Table lists the current set of portal APs. A single AP can provide all management services (enrollment, NM and security). An additional AP can provide redundant security service by mirroring the RADIUS database of the portal AP so that continuous authentication service can be provided to wireless users when the primary portal AP is undergoing maintenance.

Add Redundant Security Portal

AP IP-Address	

APPLY RESET

Portal Table

	AP	AP Device-Id	Enrollment Status
	192.168.168.24	AP_00-0A-F5-00-01-F2	Enrolled
○	192.168.168.21	AP_00-0A-F5-00-02-E2	Unenrolled

DELETE

Auto-Synchronize Databases

Sync Frequency (minutes)	□ Default Periodic 3

APPLY SYNCH DB NOW RESET

DB Version Table

AP IP Address	Radius Client DB Version	Radius User DB Version	Certificate DB Version	AP Device-ID	Enrollment Status
192.168.168.24	1.0	1.0	1.0	AP_00-0A-F5-00-01-F2	Enrolled

Perform the following functions on this tab:

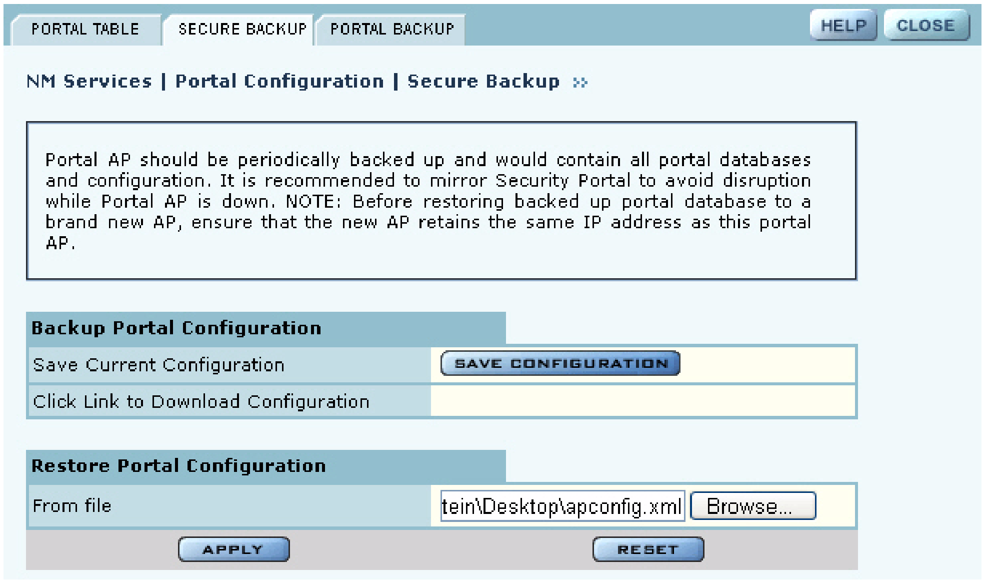
Field	Description
Add Redundant Security Portal	Specify the IP address, and click **Apply**. Only an already-enrolled AP can be configured to be a redundant security portal.
Portal Table	View the list of currently identified NM Portal APs. The listing includes the IP address of the AP, its device ID, and whether the AP is currently enrolled. To delete an entry from the table, select the radio button to the left of the entry, and click **Delete**. All Portals shown in this table as unenrolled are currently not managed by this NM Portal but form part of other managed networks. Only Portals managed by this NM Portal will be shown as Enrolled and or will have a radio button using which the portal may be deleted.

Field	Description
Sync Frequency	Select to automatically synchronize the database between the portals. The sync frequency represents the duration in minutes at which NM Portal cross checks the portals in the network to make sure their databases synchronized with the NM Portal database. Click **Apply** to save the settings, or click **Reset** to return to the default values (autonomous selected, period 5 minutes). It is recommended to accept the default value to make sure that synchronization takes place.
Portal DB Version Table	View current database information for user security. For each AP designated as a security portal, the table lists the following information: • AP IP Address—IP address of each portal AP. • RADIUS Client DB Version—Version of the user database resident on the RADIUS client. • RADIUS User DB Version—Version of the user database for RADIUS users. • Certificate DB Version—Version of the security certificate for RADIUS clients. • AP Device-ID—Unique identifier for the AP. • Enrollment Status—Indication of whether the AP is enrolled.

Secure Backup

Use the Secure Backup tab (Figure 139) to save the NM Portal database and configuration using the secure https protocol.

Figure 140: NM Services - Portal Configuration - Secure Backup



Portal AP should be periodically backed up and would contain all portal databases and configuration. It is recommended to mirror Security Portal to avoid disruption while Portal AP is down. NOTE: Before restoring backed up portal database to a brand new AP, ensure that the new AP retains the same IP address as this portal AP.

Backup Portal Configuration	
Save Current Configuration	SAVE CONFIGURATION
Click Link to Download Configuration	

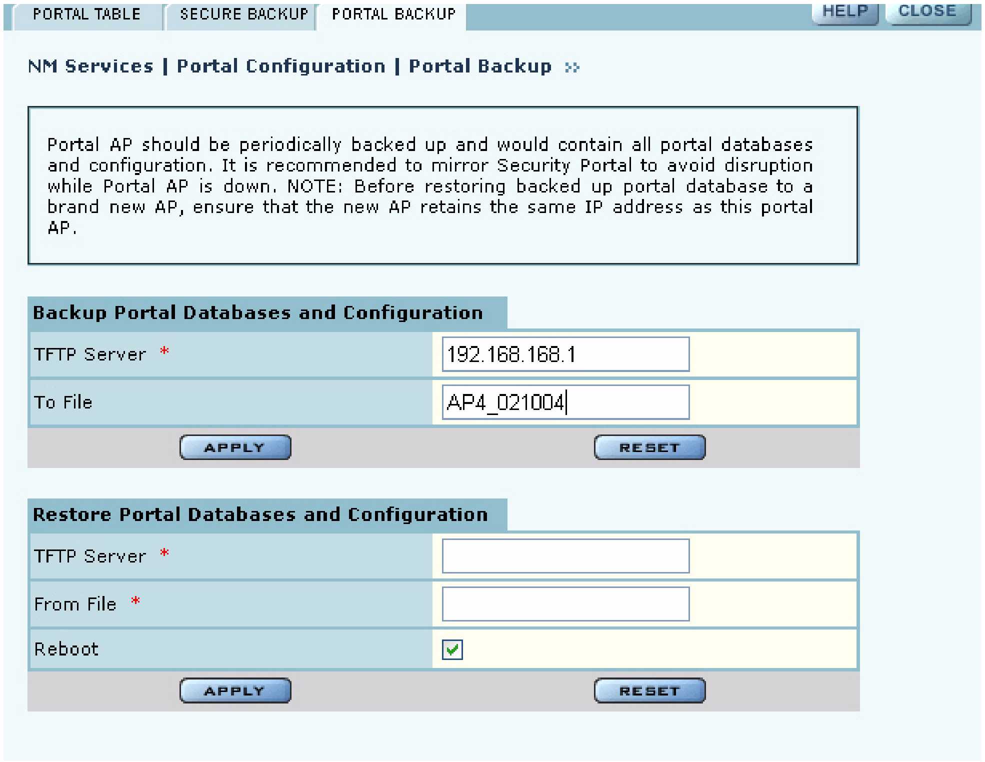
Restore Portal Configuration	
From file	tein\Desktop\apconfig.xml Browse...

Click **Save Configuration**. When the configuration is generated, a hyperlink is displayed. Right-click and select **Save As** to save the configuration locally. After the configuration file is saved, click **Delete** to remove the file from the AP. The file takes up space on the AP disk, so it is recommended to remove it. To restore the configuration, browse to select the file, and then click **Apply** to restore the configuration and reboot the AP.

Portal Backup

Use the Portal Backup tab (Figure 141) to back up the portal databases and configuration to a TFTP server and to restore the configuration from the TFTP server. For backup and restore, enter the server IP address and specify a backup file name. For restore, enter the same TFTP server address and file name. If you want to reboot the AP once the configuration file has been copied, select **Reboot**. (required)

Figure 141: NM Services - Portal Configuration - Backup/Restore



NM Services | Portal Configuration | Portal Backup »

Portal AP should be periodically backed up and would contain all portal databases and configuration. It is recommended to mirror Security Portal to avoid disruption while Portal AP is down. NOTE: Before restoring backed up portal database to a brand new AP, ensure that the new AP retains the same IP address as this portal AP.

Backup Portal Databases and Configuration

TFTP Server *	192.168.168.1
To File	AP4_021004

Restore Portal Databases and Configuration

TFTP Server *	
From File *	
Reboot	☑

Configuring the DHCP Server

NM Portal includes an internal DCHP server, which can be activated to support IP address assignments in the network if a DHCP server is not in place. Choose **DHCP** from the NM Services menu to open the DHCP panel. The panel contains four tabs:

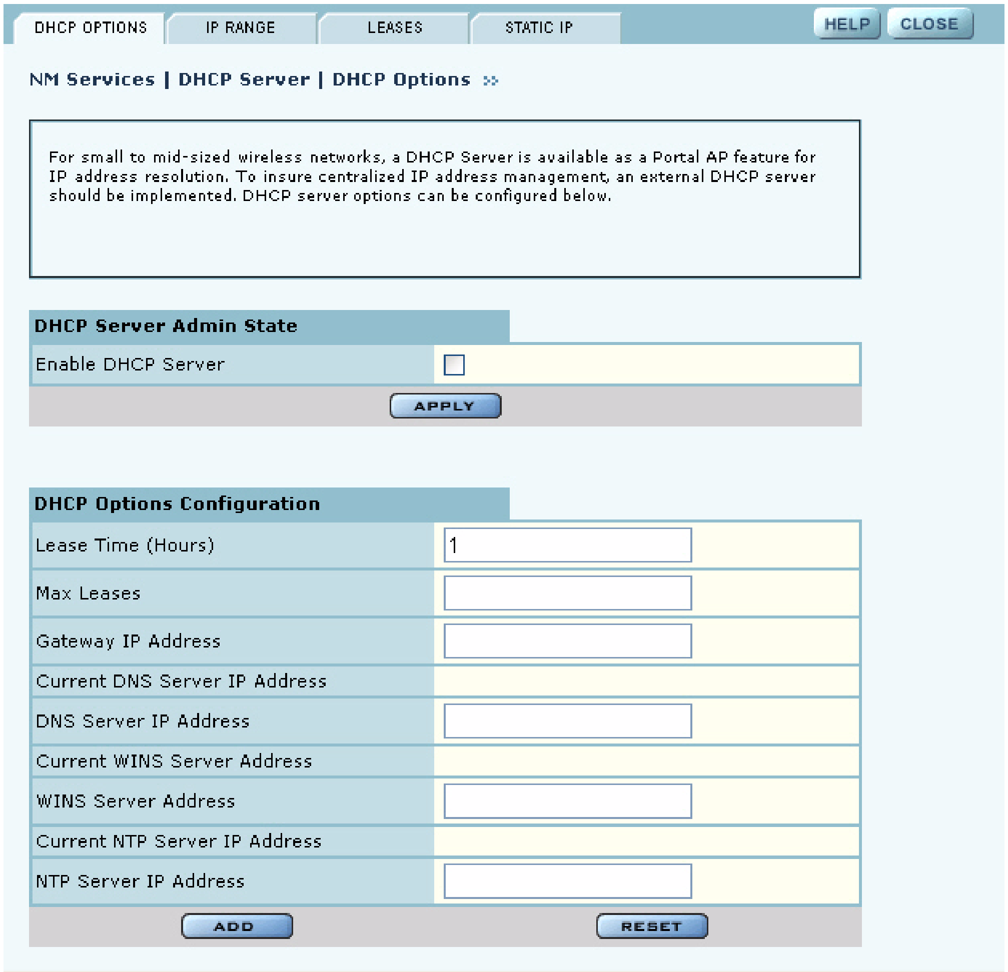
- DHCP Options—Activate and configure the DHCP server.
- IP Range—Enter address information for the DHCP server.
- Leases—View details about the current DHCP leases.
- Static IP—Assign static IP addresses for specific equipment

NOTE: Use the DHCP panels to support IP address assignments only if a DHCP server is not already in place on the existing network.

DHCP Options

Select the DHCP Options tab (Figure 142)to activate and configure the DHCP server.

Figure 142: NM Services - DHCP Configuration - DHCP Options



NM Services | DHCP Server | DHCP Options »

For small to mid-sized wireless networks, a DHCP Server is available as a Portal AP feature for IP address resolution. To insure centralized IP address management, an external DHCP server should be implemented. DHCP server options can be configured below.

DHCP Server Admin State

Enable DHCP Server	□

DHCP Options Configuration

Lease Time (Hours)	1
Max Leases	
Gateway IP Address	
Current DNS Server IP Address	
DNS Server IP Address	
Current WINS Server Address	
WINS Server Address	
Current NTP Server IP Address	
NTP Server IP Address	

To activate the server, **Enable DHCP Server** and configure the following information:

Field	Description
Lease Time	Specify the maximum number of leases that the server should assign. This is used to restrict the number of IP addresses served even though the IP subnet served by the DHCP server may be large
Maximum Leases	Specify the maximum number of available leases. There is no default.
Gateway	Enter the IP address of the gateway. There is no default.
DNS Server IP Address	Enter the IP address of the server or servers that provide domain name resolution. There is no default. More than one DNS IP address may be specified (space separated). If the field is left blank, then any previously configured DNS server addresses will be deleted. If you delete DNS servers, only those added manually are deleted. DHCP-assigned DNS servers continue to be available.
WINS Server	Enter the IP address of the Windows name server used to map IP addresses to computer names. There is no default.

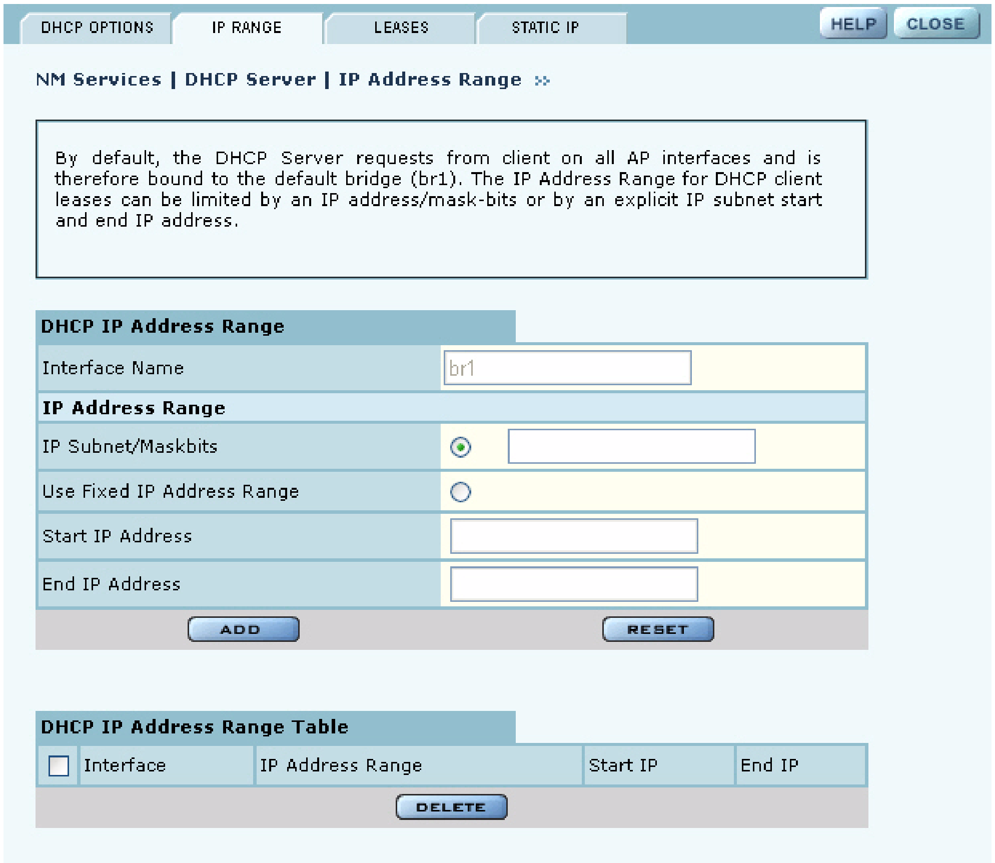
Field	Description
NTP Server	Enter the IP address of the server or servers used to synchronize network clocks. There is no default. More than one NTP IP address may be specified (space separated). If you delete NTP servers, only those added manually are deleted. DHCP-assigned NTP servers continue to be available.

Click **Add** to save the configuration information.

IP Range

Select **IP Range** to configure address ranges for DHCP leases (Figure 143).

Figure 143: NM Services - DHCP Configuration - IP Range



NM Services | DHCP Server | IP Address Range »

By default, the DHCP Server requests from client on all AP interfaces and is therefore bound to the default bridge (br1). The IP Address Range for DHCP client leases can be limited by an IP address/mask-bits or by an explicit IP subnet start and end IP address.

DHCP IP Address Range

Interface Name	br1
IP Address Range	
IP Subnet/Maskbits	●
Use Fixed IP Address Range	○
Start IP Address	
End IP Address	

ADD RESET

DHCP IP Address Range Table

□	Interface	IP Address Range	Start IP	End IP

DELETE

Enter the following information on this panel:

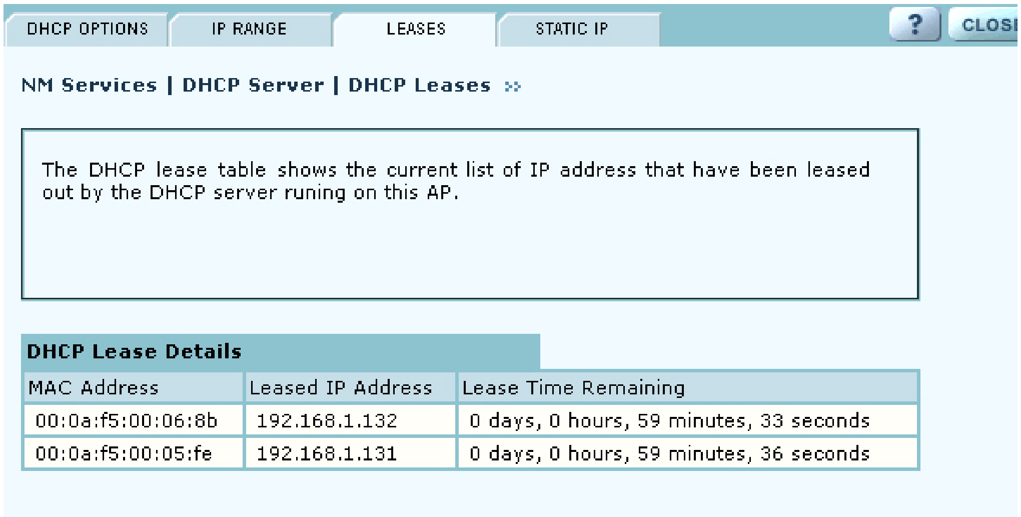
Field	Description
Interface Name	Confirm the alphanumeric name of the AP interface. The default is br1, which is the default bridge.
IP Address Range	Select a radio button to specify the range of addresses available for assignment. Choose either of the following: • IP Address/Maskbits—Enter the address and maskbits that define the subnet to be used for address assignment. • Use Fixed IP Address Range—Specify a range of IP addresses by entering starting and ending addresses, with subnet prefix length.

Click **Apply** to save the address information. Add additional interfaces if desired. The added interfaces are listed in the DHCP Address Range table at the bottom of the panel. To delete a DHCP interface, select the interface in the DHCP IP Address Range table, and click **Delete**.

Leases

The Leases tab (Figure 144) lists each network computer serviced by DHCP and its lease information.

Figure 144: NM Services - DHCP Configuration - Leases



NM Services | DHCP Server | DHCP Leases >>

The DHCP lease table shows the current list of IP address that have been leased out by the DHCP server runing on this AP.

DHCP Lease Details

MAC Address	Leased IP Address	Lease Time Remaining
00:0a:f5:00:06:8b	192.168.1.132	0 days, 0 hours, 59 minutes, 33 seconds
00:0a:f5:00:05:fe	192.168.1.131	0 days, 0 hours, 59 minutes, 36 seconds

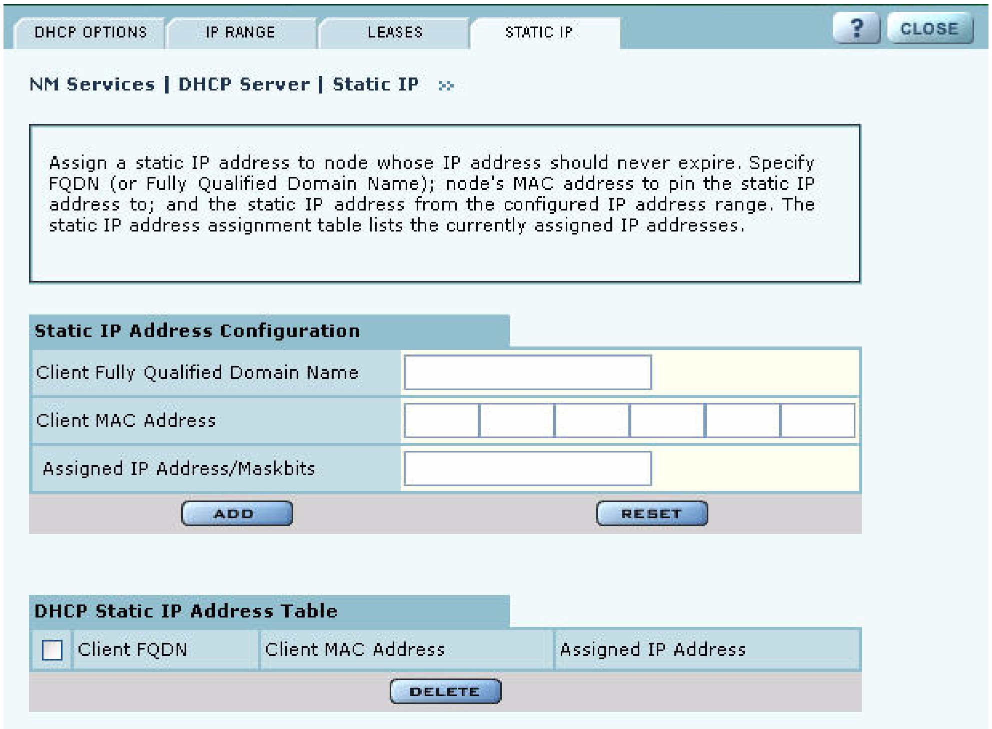
This table contains the following information:

Field	Description
MAC Address	Address that uniquely defines the DHCP client
Leased IP Address	IP address assigned by the DCHP server
Lease Time Remaining	Amount of time remaining on the current DHCP lease (in hours)

Static IP

Use the Static IP tab (Figure 145) to reserve static IP addresses for specific nodes.

Figure 145: NM Services - DHCP Configuration - Static IP



Assign a static IP address to node whose IP address should never expire. Specify FQDN (or Fully Qualified Domain Name); node's MAC address to pin the static IP address to; and the static IP address from the configured IP address range. The static IP address assignment table lists the currently assigned IP addresses.

Static IP Address Configuration

Client Fully Qualified Domain Name	
Client MAC Address	
Assigned IP Address/Maskbits	

DHCP Static IP Address Table

□	Client FQDN	Client MAC Address	Assigned IP Address

Enter the following information on this tab:

Field	Description
Fully Qualified Domain Name	Enter an alphanumeric name for the node, which is fully qualified by DNS.
Client MAC Address	Enter the MAC address that uniquely identifies the client station.
Assigned IP Address/ Maskbits	Assign the static IP address and maskbits.

Click **Add** to save the information. The new entry is listed in the table at the bottom of the tab to delete an entry, select the name in the DHCP Static IP Table, and click **Delete**.

Managing Network Faults

NM Portal aggregates alarms from all managed APs. Each AP can store up to 260 alarms locally. When the number of alarms exceeds this limit, the oldest alarms are deleted as needed. Use the Fault Management panels to view the system alarms and syslog entries. Alarms are raised as SNMP Traps, which are forwarded to the SNMP Sink Host (or Primary NMS).

Viewing Alarms

Choose **Alarm Summary** from the Fault Management menu to view counts and descriptions of alarms that occur in the network managed by NM Portal.

The Alarm Summary panel contains three tabs:

- Alarm Summary—View counts of system alarms in the managed network.
- Alarm Table—View a detailed list of alarms.
- Filter Table—Select events that should be filtered out of the reported alarm list.

Alarm Summary

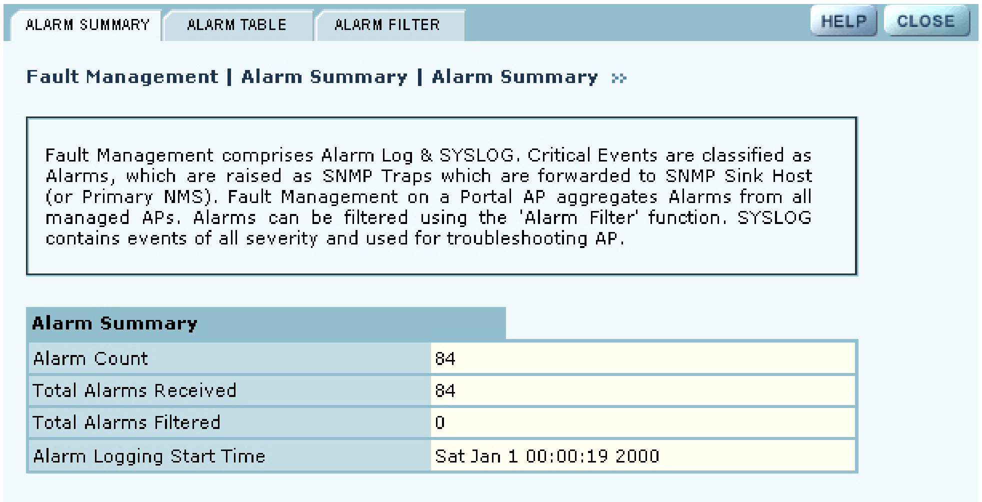
The Alarm Summary tab (Figure 146) provides an aggregate count of alarms across the network managed by NM Portal.

NOTE: The alarm count in the lower left corner of the Network Management Explorer window is the same as that given on the Alarm Summary tab. Click the Alarm Summary hyperlink to open the Alarm Summary tab.

The Alarm Summary tab contains the following information:

Field	Description
Alarm Count	Total alarms in the managed network
Total Alarms Received	Total alarms from APs other than this AP
Total Alarms Filtered	Count of alarms not displayed because they were filtered out
Alarm Logging Start Time	Time at which the counts began

Figure 146: Fault Management - Alarm Summary



Fault Management | Alarm Summary | Alarm Summary »

Fault Management comprises Alarm Log & SYSLOG. Critical Events are classified as Alarms, which are raised as SNMP Traps which are forwarded to SNMP Sink Host (or Primary NMS). Fault Management on a Portal AP aggregates Alarms from all managed APs. Alarms can be filtered using the 'Alarm Filter' function. SYSLOG contains events of all severity and used for troubleshooting AP.

Alarm Summary	
Alarm Count	84
Total Alarms Received	84
Total Alarms Filtered	0
Alarm Logging Start Time	Sat Jan 1 00:00:19 2000

Alarm Table

The Alarm Table tab (Figure 147) provides a detailed description of alarms and enables filtering of the alarm table for easy viewing and searching. A description of all the alarms is provided in “108Mbps Wireless LAN Access Point Alarms” on page 198 and additional details are presented in Appendix C, “Alarms.”.

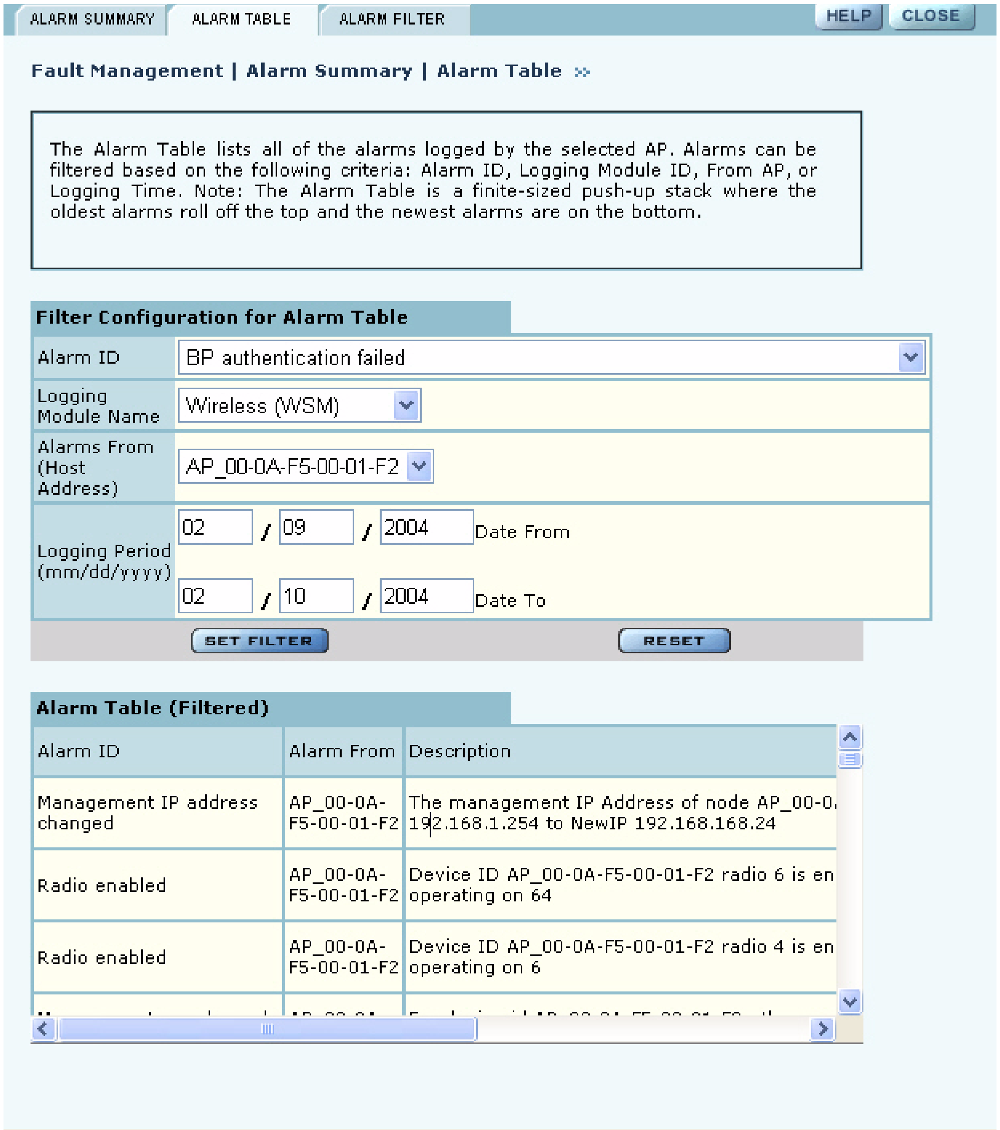
The Alarm Table includes the following information:

Field	Description
Alarm ID	Text description of the specific alarm

Field	Description
Alarm From	Device ID of the AP that reported the alarm
Description	Text description of the event
Log Time	Time the alarm occurred and was logged
From Module	The subsystem that is the source of the alarm. Modules include: • Authentication • Networking • Distribution • Configuration • Wireless • Discovery • NM Portal • SW Download

NOTE: The filtering function on the Alarm Table tab only affects the information that is displayed in the Alarm Table at the bottom of the tab. To remove some event types completely from the alarm list, use the Alarm Filter tab.

Figure 147: Fault Management - Alarm Summary - Alarm Table



Fault Management | Alarm Summary | Alarm Table »

The Alarm Table lists all of the alarms logged by the selected AP. Alarms can be filtered based on the following criteria: Alarm ID, Logging Module ID, From AP, or Logging Time. Note: The Alarm Table is a finite-sized push-up stack where the oldest alarms roll off the top and the newest alarms are on the bottom.

Filter Configuration for Alarm Table

Alarm ID	BP authentication failed
Logging Module Name	Wireless (WSM)
Alarms From (Host Address)	AP_00-0A-F5-00-01-F2
Logging Period (mm/dd/yyyy)	02 / 09 / 2004 Date From 02 / 10 / 2004 Date To

Alarm Table (Filtered)

Alarm ID	Alarm From	Description
Management IP address changed	AP_00-0A-F5-00-01-F2	The management IP Address of node AP_00-0 192.168.1.254 to NewIP 192.168.168.24
Radio enabled	AP_00-0A-F5-00-01-F2	Device ID AP_00-0A-F5-00-01-F2 radio 6 is en operating on 64
Radio enabled	AP_00-0A-F5-00-01-F2	Device ID AP_00-0A-F5-00-01-F2 radio 4 is en operating on 6

Configure the following fields to define a viewing filter:

Field	Description
Alarm ID	Select an alarm from the list to view only those specific alarms.
Logging Module Name	Select from the list to filter all the alarms from a specific system logging module.
Alarms From (Host Address)	Select an AP to view only the alarms generated by that AP.
Logging Period	Enter a date range to show events during a specific interval of time.

Click **Set Filter** to apply the filter to the alarm table or **Reset** to clear the selected values.

Table 14: 108 Mbps Wireless Access Point Alarms

Alarm ID	Description
Discovered new node	Generated when a new 108 Mbps Wireless Access Point is discovered by NM Portal for the first time.
Node deleted from network	Generated when a previously-discovered node is deleted from the system. When the node is deleted, all information about that node is deleted from NM Portal. If the node's IP address falls within the discovery scope, then the node will be re-discovered and added back to the set of the discovered nodes during the next discovery scan.
Managed nodes limit exceeded	Generated when the number of discovered nodes exceeds the limit defined in the Discovery Configuration panel, Configuration tab. See "Configuring Network Discovery" on page 184). If this alarm occurs, NM Portal ceases to discover nor track any new nodes.
Node Enrolled	Generated when an 108 Mbps Wireless AP has been successfully enrolled.
Node Un-Enrolled	Generated when an 108 Mbps Wireless AP has been successfully rejected (un-enrolled).
Policy Download Successful	Generated when a policy is successfully downloaded to an AP.
Policy Download Failed	Generated when policy downloaded to an AP is unsuccessful due to an error in the policy, software version mismatch, or other error.
Image download succeeded.	Generated when an image is successfully downloaded and applied to an AP.
Image download failed	Generated when image download to an AP is unsuccessful, due to corrupted images, images of invalid length, or connectivity failures.
Software distribution succeed	Generated when an image distribution is completed.
Radio enabled (BSS Enabled)	Generated when a AP radio is enabled. Indicates successful start of a BSS and includes the channel on which the AP radio will be operating.
Radio Disabled (BSS disabled)	Generated when an AP is disabled. Disabling can be user triggered for administrative purposes, caused by radio reset due to application of wireless configuration parameters, triggered by hardware, or due to a change in SSID.
BSS Enabling Failed	Generated when an attempt to enable an AP radio fails. Reason codes: 0 – Unspecified reason 1 – System timeout attempting to enable BSS

Table 14: 108 Mbps Wireless Access Point Alarms (continued)

Alarm ID	Description
Frequency Changed	Generated when operating frequency is changed for an AP radio due to user intervention or events such as periodic dynamic frequency selection (DFS). Reason Codes: 0 - Triggered due to DFS 1 - User Triggered
STA Association Failed	Generated when a 802.11 client station fails in its attempt to associate to the AP radio. Reason Codes: 1 **-** Invalid parameters received from station in association request 2 - Only stations are allowed to associate with this AP based on current configuration 3 - Only backhauls can be formed with this AP based on current configuration 4 - Max backhaul limit is reached based on the 'Max Trunks' configuration for AP Admission Criteria 5 - Max station limit is reached based on the 'Max Stations' configuration for SSID 6 - SSID received in association request does not match SSID in AP configuration. This can occur more often when AP is not broadcasting SSID in beacon (due to suppressed SSID or multiple SSIDs being configured) and station is associating with AP with a different SSID. 7 - Authentication and encryption requested by station does not match security policy of the AP 8 - Multi Vendor Station are not allowed to associate based on AP Admission Criteria 9 - 802.11b stations are not allowed to associate based on AP Admission Criteria 10 - Station is not allowed to associate and transferred to another AP Radio due to Load Balancing 11 - Station is not allowed to associate because node does not have network connectivity
STA Associated	Generated when a client station succeeds in associating to the AP radio. The alarm message includes the current associated stations, type of association and user ID. The user ID is the user name if RADIUS authentication is used and the MAC address otherwise.
STA Disassociated	Generated when a 802.11 station is disassociated by the network or the station. Reason Codes: 0 - Station initiated disassociation 1 - Station has handed off to another AP 2 - Disassociation triggered due to authentication failure after ULAP timeout 3 - Disassociation triggered due to user action

Table 14: 108 Mbps Wireless Access Point Alarms (continued)

Alarm ID	**Description**
WDS Failed	Generated when wireless backhaul formation fails. The message includes the MAC address of the end node. This alarm can help track losses in network connectivity. Reason Codes: 0 - System Failure 1 - Maximum BP count has been reached (this relevant only for AP) 2 - Join attempt to the uplink AP failed (BP side only)
WDS Up	Generated when a wireless backhaul formation succeeds. The message includes the MAC address of the end node. Reason Codes: 0 - Trunk has been established 1 - Trunk has been optimized (re-established based on better connectivity)
WDS Down	This is a notification generated when a wireless backhaul has gone down. The remote end's MAC address is provided. Reason Codes: 0 - System Reason (unspecified) 1 - Loss of Link (applies to BP side only) 2 - Trunk brought down by uplink AP (applies to BP side only) 3 - User retrunk issued (this can occur due to new backhaul configuration being applied on BP) 4 - Trunk has reformed with another AP (AP side only) 5 - Trunk brought down by BP (applies to AP side only)
Guest Authentication Succeeded	Generated when a guest station is authenticated, and indicates the successful start of a guest access communications session. The guest user is offered the communications services specified in the guest profile for the specified SSID.
Guest Authentication Failed	Generated when a guest station fails authentication.
User Reject by RADIUS Server	Generated when user authentication fails. The AP radio and the RADIUS server which rejected the user are included in the message.
BP rejected by RADIUS Server	Generated when security portal has rejected the attempt by a BP radio to associate to the AP. This may mean that the BP is not enrolled in the same network as the AP or that the BP was just enrolled, but the enrollment database has not yet been synchronized across the network to all security portals.
RADIUS Server timeout	Generated when the RADIUS server fails to respond within the RADIUS timeout period. The RADIUS server may be unreachable over the network, or the shared secret for the RADIUS server is incorrectly configured on the AP. If multiple RADIUS servers are configured in this authentication zone, the AP will switch to using the next one in the list.

Table 14: 108 Mbps Wireless Access Point Alarms (continued)

Alarm ID	Description
Management User login success	Generated when a management user successfully logs in to the local AP.
Management User login failure	Generated when a management user fails to log in to the AP.
STA failed EAPOL MIC check	Generated when the MIC fails during EAPOL key exchange process. If the authentication type is WPA PSK and the failure happened during the pairwise key exchange, then the most likely reason is incorrect configuration of the WPA PSK on the station. It could also mean that an attacker's station is attempting to masquerade as a legal station.
STA attempting WPA-PSK – no Pre-shared Key is set for SSID	Generated when a client station attempts to perform WPA-PSK based authentication on a given SSID, but no WPA pre-shared key has been configured for that SSID.
Auth Server Improperly configured on this SSID	Generated when the AP has determined that a station requires an authentication server, but none is configured for this SSID. Authentication servers are needed for EAP based authentication and MAC address based ACL lookups.
STA failed to send EAPOL-Start	Generated when the AP has determined that a client station has failed to send an EAPOL-Start, possibly indicating incorrect configuration of the station. The AP expects the station to send an EAPOL-Start if the authentication type is deemed to be EAP based. This can happen when WPA EAP authentication is negotiated, or when WEP is enabled on the AP and no manual WEP keys are configured.
RADIUS sent a bad response	Generated during authentication, when the RADIUS server sends a bad or unexpected response. This would occur if the cryptographic signature check failed or an attribute is missing or badly encoded.
RADIUS timeout too short	Generated when the AP receives a late response from the RADIUS server, generally due to high network latencye. The AP may have attempted multiple retries or may have switched to another RADIUS server by this time. If this alarm is generated repeatedly, it may be desirable to increase the timeout associated with the authentication server.
STA authentication did not complete in time	Generated when the station authentication sequence did not complete in time.
Upstream AP is using an untrusted auth server	Generated when the local BP determines that the upstream AP is using an untrustworthy authentication server. This could mean that the upstream AP is a rogue AP. If the downstream AP was previously enrolled in another network, it should be rest and re-enrolled in the new network.
Upstream AP is using a non-portal node as its auth server	Generated when the local BP determines that the upstream AP is using a node that is not a security portal as its authentication server. The BP is aware of the other PLANEX node, but does not believe it is authorized to be a security portal.
Upstream AP failed MIC check during BP authentication	Generated when the MIC fails during EAPOL key exchange process with a BP radio.

Table 14: 108 Mbps Wireless Access Point Alarms (continued)

Alarm ID	Description
Premature EAP-Success receive	Generated when an upstream AP sends an EAP success before authentication is complete. This may indicate that a rogue AP is trying to force an AP to join before authentication is complete.
Profile not configured for user-group	Generated when the AP determines that the station is a member of a group that does not have a service profile defined for this SSID.
STA has failed security enforcement check	Generated if the station attempts to use an encryption type that is not allowed in its service profile. The AP can advertise multiple encryption capabilities, but different stations may be restricted to different subsets of encryption capabilities based on their service profiles.
AP Detected Bad TKIP MIC	Generated when a bad TKIP MIC is detected on an incoming frame from a station that is encrypted with a pairwise/unicast key. All packets received by the AP are always encrypted with the pairwise/unicast key.
BP detected Bad TKIP MIC on Incoming Unicast	Generated when a bad TKIP MIC is detected by a local BP radio on an incoming frame encrypted with the pairwise/ unicast key.
BP detected Bad TKIP MIC on Incoming Multicast/Broadcast	Generated when a bad TKIP MIC is detected by a local BP radio on an incoming multicast or broadcast packet from the AP, where the packet is encrypted with the group/multicast/ broadcast key.
STA detected Bad TKIP MIC on Incoming Unicast	Generated when a bad TKIP MIC is detected by an station associated with this AP on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.
STA detected Bad TKIP MIC on Incoming Multicast/Broadcast	Generated when a bad TKIP MIC is detected by an station associated with a radio on an incoming multicast or broadcast packet from the AP, where the packet is encrypted with the group/multicast/broadcast key.
TKIP counter-measures lockout period started	Generated when a TKIP counter measures lockout period for 60 seconds is started. Indicates that the AP has determined that an attempt is underway to compromise the secure operation of TKIP. This happens if two MIC failures are detected within a 60 second interval. If this happens, the AP disassociates all stations and prevents new stations from associating for a period of 60 seconds.
EAP User-ID timeout	Generated when a station fails to send its user-ID in time to complete its authentication sequence using the specified authentication type. The two authentication modes that require the station to send its user-ID are WPA EAP and legacy 8021.x for dynamic WEP. This alarm may indicate that a user prompt is not attended to on the client side.

Table 14: 108 Mbps Wireless Access Point Alarms (continued)

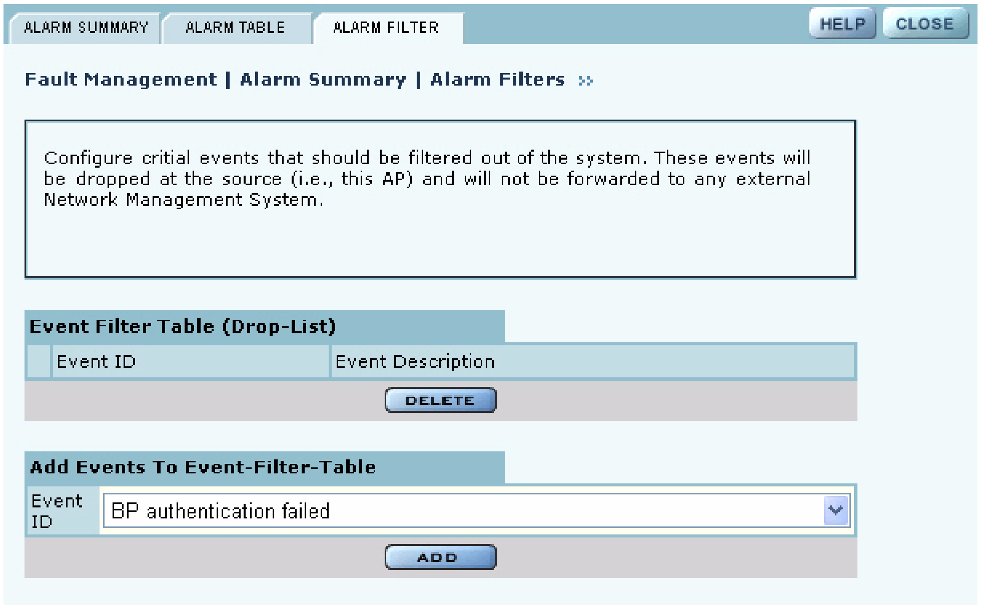
Alarm ID	Description
EAP response timeout	Generated when a station fails to send an EAP-Response in time to complete its authentication sequence using the specified authentication type and encryption. The two authentication modes that require the station to send EAP responses are WPA EAP and legacy 8021.x for dynamic WEP. This alarm may mean that a user prompt is not attended to on the client side. It may also indicate that the client silently rejected a EAP request sent from the RADIUS server – perhaps because it did not trust the RADIUS server's credentials.
EAPOL Key exchange – message 2 timeout	Generated when a station fails to send the WPA EAPOL-Key Pairwise Message #2 in time to complete the pairwise key exchange.
EAPOL Key exchange – message 4 timeout	Generated when a station fails to send the WPA EAPOL-Key Pairwise Message #4 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.
EAPOL Group 2 key exchange timeout	Generated when a station fails to send the WPA EAPOL-Key Group Message #2 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.

Alarm Filter

Use the Alarm Filter tab (Figure 148) to eliminate selected events from the alarm displays in the Alarm Summary and Alarm Table tabs.

Select an event ID from the list, and click **Add** to include the event type in the list of events that are not reported. Each added event is included in the Event Filter Table Drop List at the top of the tab.The table includes the event ID and a description. To remove an event from the list, select the event, and click **Delete**.

Figure 148: Fault Management - Alarm Summary - Alarm Filter



Fault Management | Alarm Summary | Alarm Filters »

Configure critial events that should be filtered out of the system. These events will be dropped at the source (i.e., this AP) and will not be forwarded to any external Network Management System.

Event Filter Table (Drop-List)

	Event ID	Event Description

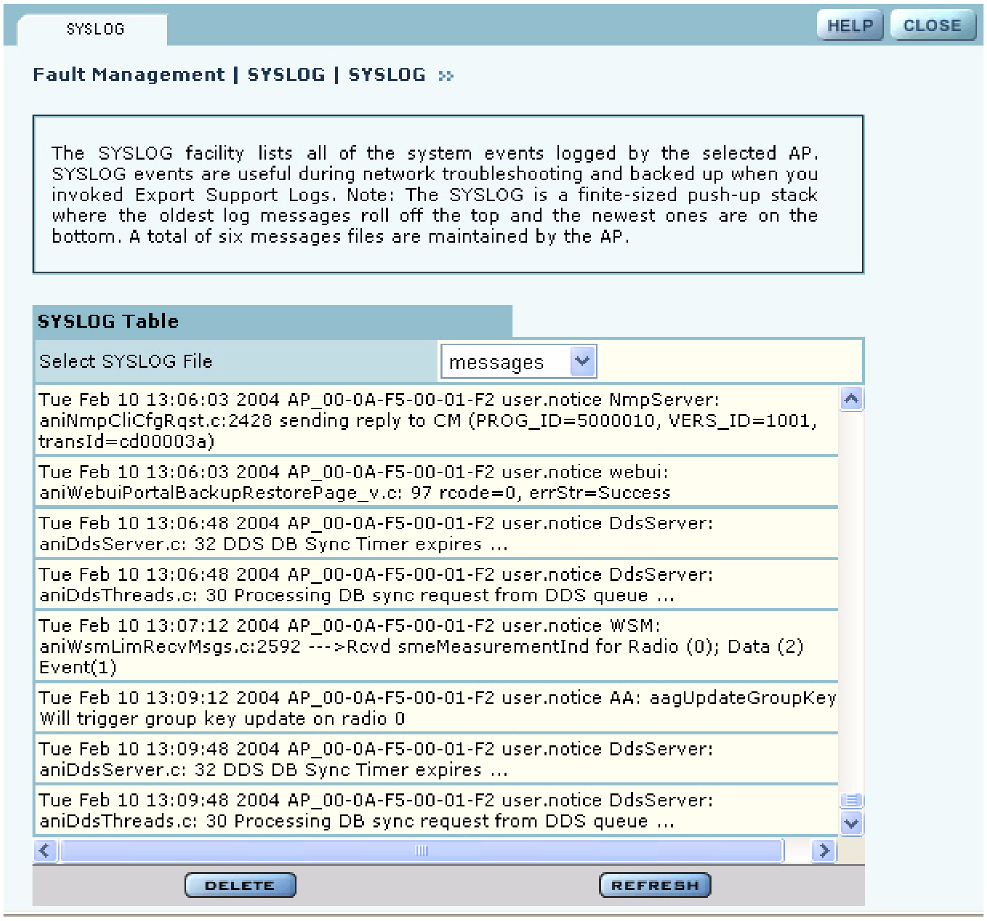
Add Events To Event-Filter-Table

Event ID	BP authentication failed

Viewing the Syslog

Select SYSLOG from the Fault Management menu to view syslog messages used for network troubleshooting. The most recent messages are in the default message file, `Messages`, with the latest messages at the top. To view older messages, select the appropriate `message.x` file from the list on the SYSLOG panel (Figure 149). See “Syslog Configuration” on page 213 for instructions on configuring the syslog message output.

Figure 149: Fault Management - SYSLOG



The SYSLOG facility lists all of the system events logged by the selected AP. SYSLOG events are useful during network troubleshooting and backed up when you invoked Export Support Logs. Note: The SYSLOG is a finite-sized push-up stack where the oldest log messages roll off the top and the newest ones are on the bottom. A total of six messages files are maintained by the AP.

SYSLOG Table

Select SYSLOG File: messages

```
Tue Feb 10 13:06:03 2004 AP_00-0A-F5-00-01-F2 user.notice NmpServer:
aniNmpCliCfgRqst.c:2428 sending reply to CM (PROG_ID=5000010, VERS_ID=1001,
transId=cd00003a)
Tue Feb 10 13:06:03 2004 AP_00-0A-F5-00-01-F2 user.notice webui:
aniWebuiPortalBackupRestorePage_v.c: 97 rcode=0, errStr=Success
Tue Feb 10 13:06:48 2004 AP_00-0A-F5-00-01-F2 user.notice DdsServer:
aniDdsServer.c: 32 DDS DB Sync Timer expires ...
Tue Feb 10 13:06:48 2004 AP_00-0A-F5-00-01-F2 user.notice DdsServer:
aniDdsThreads.c: 30 Processing DB sync request from DDS queue ...
Tue Feb 10 13:07:12 2004 AP_00-0A-F5-00-01-F2 user.notice WSM:
aniWsmLimRecvMsgs.c:2592 --->Rcvd smeMeasurementInd for Radio (0); Data (2)
Event(1)
Tue Feb 10 13:09:12 2004 AP_00-0A-F5-00-01-F2 user.notice AA: aagUpdateGroupKey
Will trigger group key update on radio 0
Tue Feb 10 13:09:48 2004 AP_00-0A-F5-00-01-F2 user.notice DdsServer:
aniDdsServer.c: 32 DDS DB Sync Timer expires ...
Tue Feb 10 13:09:48 2004 AP_00-0A-F5-00-01-F2 user.notice DdsServer:
aniDdsThreads.c: 30 Processing DB sync request from DDS queue ...
```

Managing Users

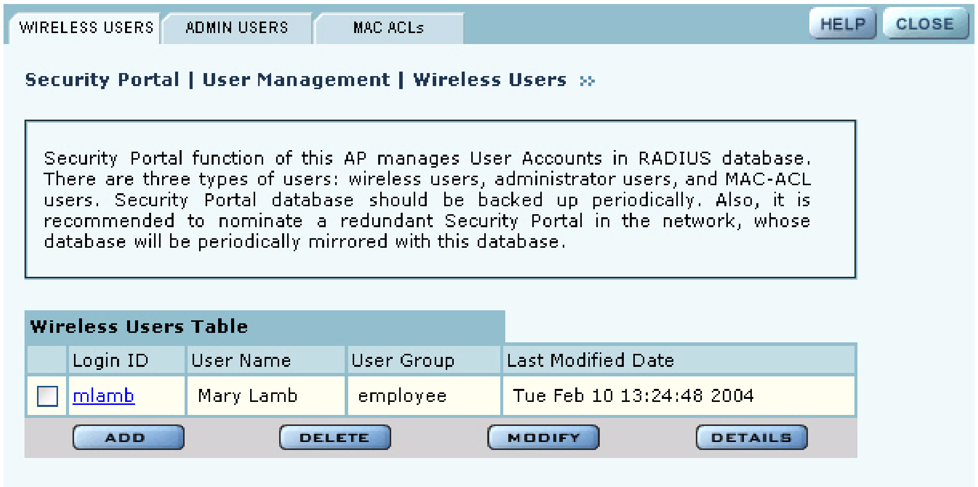
Choose **User Management** from the Security Portal menu to manage the authentication of users by way of the internal RADIUS database on the NM Portal AP. The panel contains three tabs:

- Wireless Users—Manage users who seek access to the wireless network.
- Admin Users—Manage administrators responsible for the wireless network.
- MAC ACLs—Identify and manage users using the MAC addresses of their computers.
- Guest User—Set up automatic password generation for guest users. For a description of this tab, see “Configuring Guest Access” on page 155.

Adding Wireless Users

Choose **User Management** from the Security Portal menu to open the Wireless Users tab, which contains a list of current network users (Figure 150).

Figure 150: Security Portal - User Management - Wireless Users



Security Portal | User Management | Wireless Users »

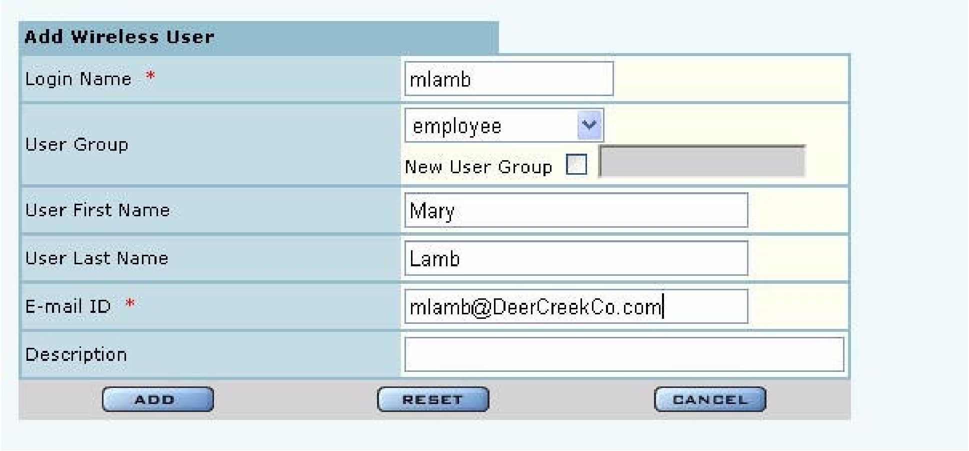
Security Portal function of this AP manages User Accounts in RADIUS database. There are three types of users: wireless users, administrator users, and MAC-ACL users. Security Portal database should be backed up periodically. Also, it is recommended to nominate a redundant Security Portal in the network, whose database will be periodically mirrored with this database.

Wireless Users Table

	Login ID	User Name	User Group	Last Modified Date
□	mlamb	Mary Lamb	employee	Tue Feb 10 13:24:48 2004

To add a new user, click **Add** to open the Add Wireless User entry panel (Figure 151).

Figure 151: Security Portal - User Management - Add Wireless User



Add Wireless User

Login Name *	mlamb
User Group	employee New User Group □
User First Name	Mary
User Last Name	Lamb
E-mail ID *	mlamb@DeerCreekCo.com
Description	

Enter the following information:

Field	Description
Login Name	Assign a login name for network access (required).
User Group	Select a user group as defined in the RADIUS server.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Email ID	Enter the user’s email address.
Description	Enter a text description, if desired.

Click **Add** to save the user record, **Reset** to clear the fields on the panel, or **Cancel** to return to the Wireless tab without saving the record.

When a wireless user is added to the database a unique certificate is generated for that user. The certificate must be installed on the user's PC. This can be done in one of two ways:

- **Email.** If an SMTP server is configured, then the certificate is mailed to the user. To install the emailed certificate on the PC:

  a Ask the administrator for the password associated with the certificate. This password is displayed in the user details page.

  b Double click on the certificate obtained through email. When the certificate installation wizard asks for the password, supply the previously-obtained password.

- **Download.** To download the certificate:

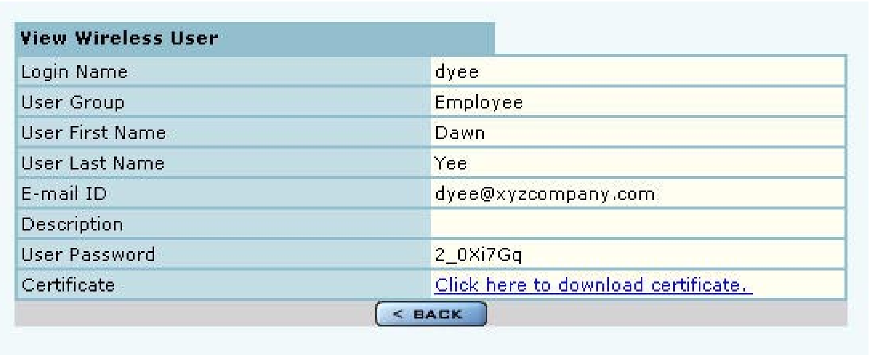
  a Click the Wireless Users tab to display the list of users.

  b Click the login name link for the user, or highlight the checkbox to the left of the Login Name, and click **Details**. This opens the View Wireless User panel (Figure 152).

  c Click the link entitled **Click Here to Download Certificate**. A security certificate pop-up opens with a prompt to open or save the certificate.

  d Save the certificate on your local computer.

Figure 152: Security Portal - User Management - View Wireless User



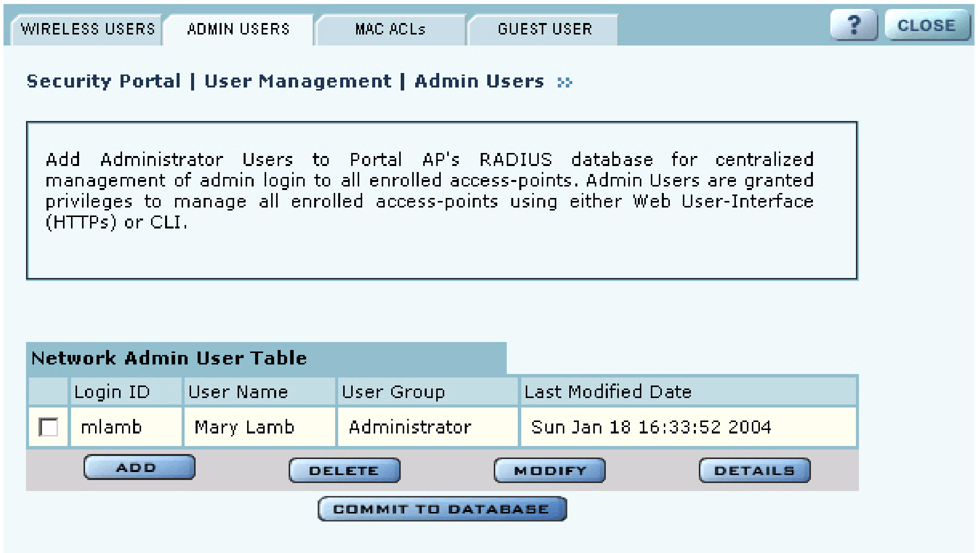
View Wireless User

Login Name	dyee
User Group	Employee
User First Name	Dawn
User Last Name	Yee
E-mail ID	dyee@xyzcompany.com
Description	
User Password	2_0Xi7Gq
Certificate	Click here to download certificate.

Adding Administrative Users

To give designated users access to NM Portal, open the Admin Users tab (Figure 153).

Figure 153: Security Portal - User Management - Admin Users



Security Portal | User Management | Admin Users »

Add Administrator Users to Portal AP's RADIUS database for centralized management of admin login to all enrolled access-points. Admin Users are granted privileges to manage all enrolled access-points using either Web User-Interface (HTTPs) or CLI.

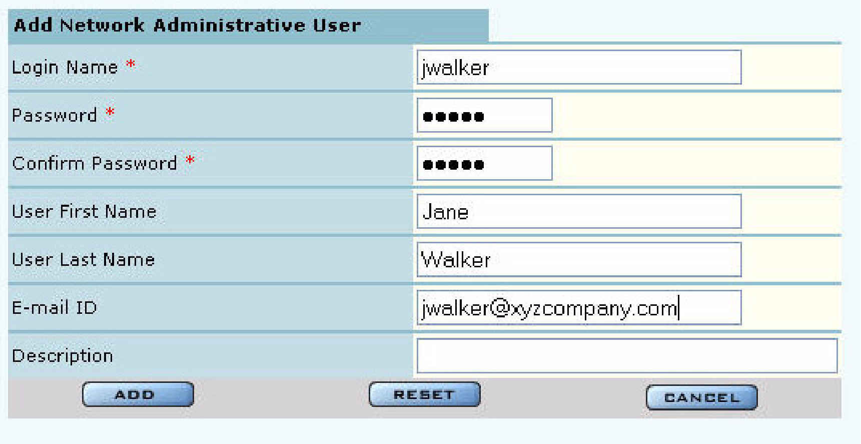
Network Admin User Table

	Login ID	User Name	User Group	Last Modified Date
□	mlamb	Mary Lamb	Administrator	Sun Jan 18 16:33:52 2004

The tab opens with a list of current administrative users. To add a new user, click **Add**, and enter the following information in the Add Administrative User entry panel (Figure 154):

Field	Description
Login Name	Assign a login name for network access (required).
Password	Enter the password and enter it again in the Confirm Password field (required).
User First Name	Enter the first name of the user.
User Last Name	Enter the last name of the user.
Email ID	Enter the user's email address.
Description	Enter a text description.

Figure 154: Security Portal - User Management - Add Administrative User



Add Network Administrative User

Login Name *	jwalker
Password *	●●●●●
Confirm Password *	●●●●●
User First Name	Jane
User Last Name	Walker
E-mail ID	jwalker@xyzcompany.com
Description	

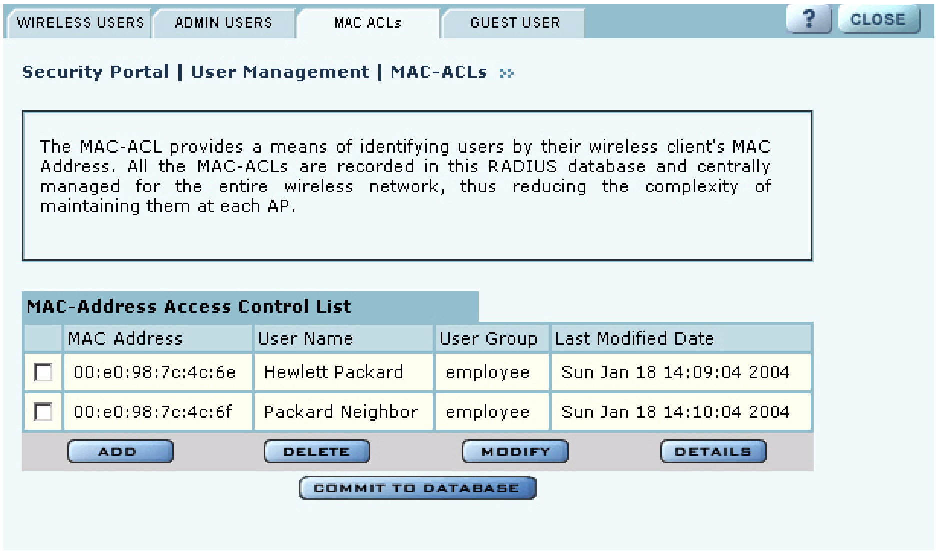
After entering the requested information, click **Add**.

From the user list, you can also delete an existing user, modify user information, or view the details in a read-only table.

Adding MAC-ACL Users

Use the MAC-ACL tab (Figure 155) to identify and authenticate users by the MAC address of the computer rather than by login. This type of authentication is generally used to accommodate legacy equipment that does not support user-based authentication. MAC addresses are checked when the SSID has MAC-ACL enabled, and open access, static WEP keys, or WPA-PSK encryption are used. For more information on security options, see Chapter 7, "Managing Security."

Figure 155: Security Portal - User Management - MAC-ACLs



Security Portal | User Management | MAC-ACLs »

The MAC-ACL provides a means of identifying users by their wireless client's MAC Address. All the MAC-ACLs are recorded in this RADIUS database and centrally managed for the entire wireless network, thus reducing the complexity of maintaining them at each AP.

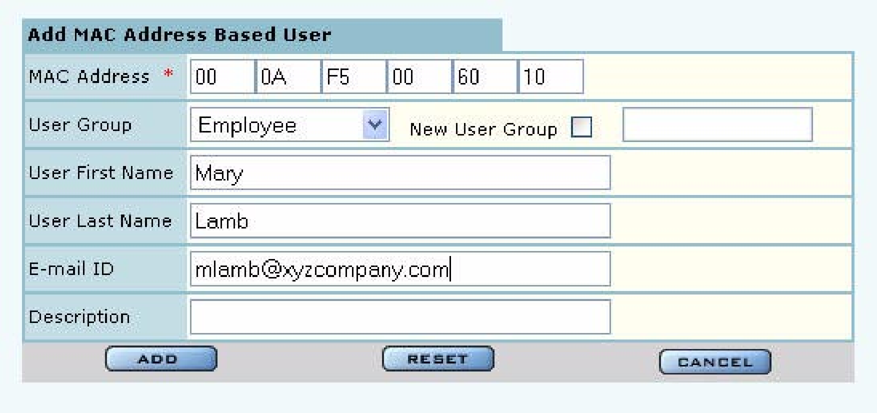
MAC-Address Access Control List

	MAC Address	User Name	User Group	Last Modified Date
□	00:e0:98:7c:4c:6e	Hewlett Packard	employee	Sun Jan 18 14:09:04 2004
□	00:e0:98:7c:4c:6f	Packard Neighbor	employee	Sun Jan 18 14:10:04 2004

The tab opens with a list of current MAC-ACL users. To add a new user, click **Add** and enter the following information in the Add MAC Address User entry panel (Figure 156):

Field	**Description**
MAC Address	Enter the MAC address that uniquely identifies the device. Use the tab key to move between the successive two-character fields (required).
User Group	Select a group from the list or create a new group.
User First Name	Enter the first name of the user.
User Last Name	Enter the last name of the user.
Email ID	Enter the user’s email address.
Description	Enter a text description, if desired.

Figure 156: Security Portal - User Management - Add MAC Address User



Add MAC Address Based User

MAC Address *	00 0A F5 00 60 10
User Group	Employee New User Group □
User First Name	Mary
User Last Name	Lamb
E-mail ID	mlamb@xyzcompany.com
Description	

Click **Add** after entering the requested information.

From the user list, you can delete an existing MAC-ACL user, modify user information, or view the details in a read-only table.

10 Maintaining the Access Point

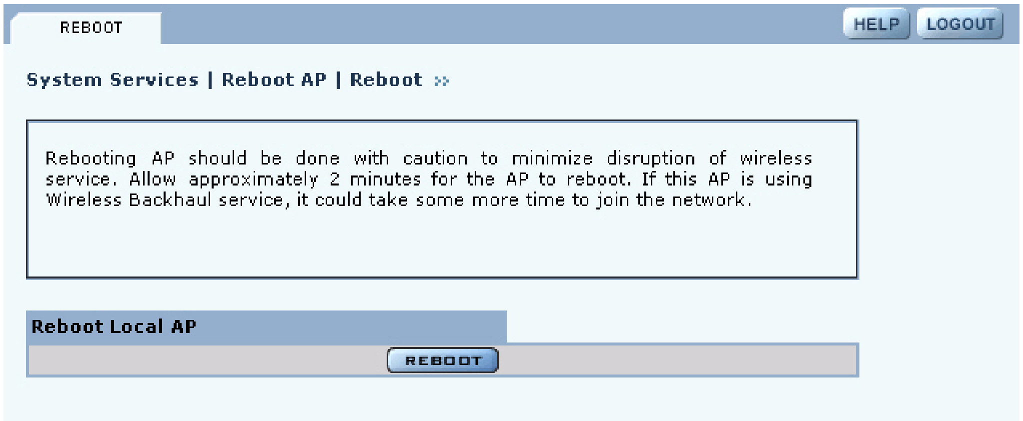
This chapter describes the tools available to maintain the 108 Mbps Wireless Access Point. It contains the following sections:

- **Rebooting the AP**
- **Managing the System Configuration**
- **Click Apply to save the entries or Reset to return to the previously saved values.**
- **Upgrading Software**
- **Common Problems and Solutions**

Rebooting the AP

Choose **Reboot AP** from the System Services menu to order a reboot of the access point. To begin the process, click **Reboot** (Figure 158). The process takes approximately 2 minutes, and may take additional time if the AP is currently used for wireless backhaul service.

Figure 157: System Configuration - Reboot AP



Rebooting AP should be done with caution to minimize disruption of wireless service. Allow approximately 2 minutes for the AP to reboot. If this AP is using Wireless Backhaul service, it could take some more time to join the network.

Managing the System Configuration

Choose **System Configuration** from the System Services menu to access the network-related configuration features of the 108 Mbps Wireless AP and set up syslog parameters.

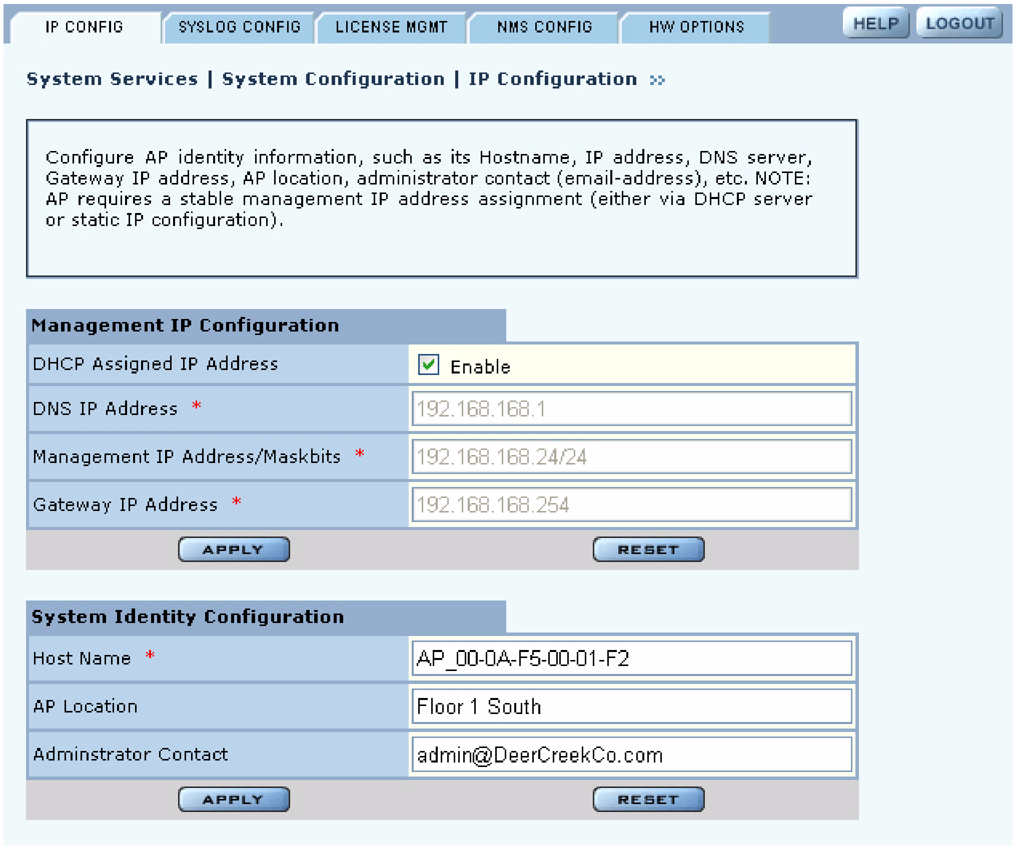
The panel includes the following tabs:

- IP Configuration—Configure IP and host settings.
- Syslog Configuration—Set up and view the syslog.
- License Management—Set up the real time clock (RTC) to keep track of time in the event that power is lost to the AP.
- NMS Configuration—Specify the entities used for network management, including the Wireless LAN Network Management Software server and NM Portal AP.
- Hardware Options—Enable the real time clock and buzzer.

IP Configuration

Use the IP Configuration tab (Figure 158) to update the IP and basic system configuration for the 108 Mbps Wireless AP.

Figure 158: System Configuration - IP Configuration



System Services | System Configuration | IP Configuration »

Configure AP identity information, such as its Hostname, IP address, DNS server, Gateway IP address, AP location, administrator contact (email-address), etc. NOTE: AP requires a stable management IP address assignment (either via DHCP server or static IP configuration).

Management IP Configuration	
DHCP Assigned IP Address	☑ Enable
DNS IP Address *	192.168.168.1
Management IP Address/Maskbits *	192.168.168.24/24
Gateway IP Address *	192.168.168.254

System Identity Configuration	
Host Name *	AP_00-0A-F5-00-01-F2
AP Location	Floor 1 South
Adminstrator Contact	admin@DeerCreekCo.com

The tab is divided into two sections. Click **Apply** after configuring each section, or **Reset** to return to the default values. Configure the following fields:

Field	Description
DHCP Assigned IP address	Enables the AP to obtain an IP address for the AP from the network DHCP server.
DNS IP Address	Enter the IP address of the DNS server. (required)
Management IP address /Maskbits	Enter the IP address and subnet prefix of the management server. (required)
Gateway IP address	Enter the IP address of the network gateway. (required)
Host Name	Enter a unique name for the AP. The default is the device ID, which is derived from the MAC address. (required)
AP Location	Enter a text description of the physical location of the AP.
Administrator Contact	Enter the email address of the administrative contact for the AP.

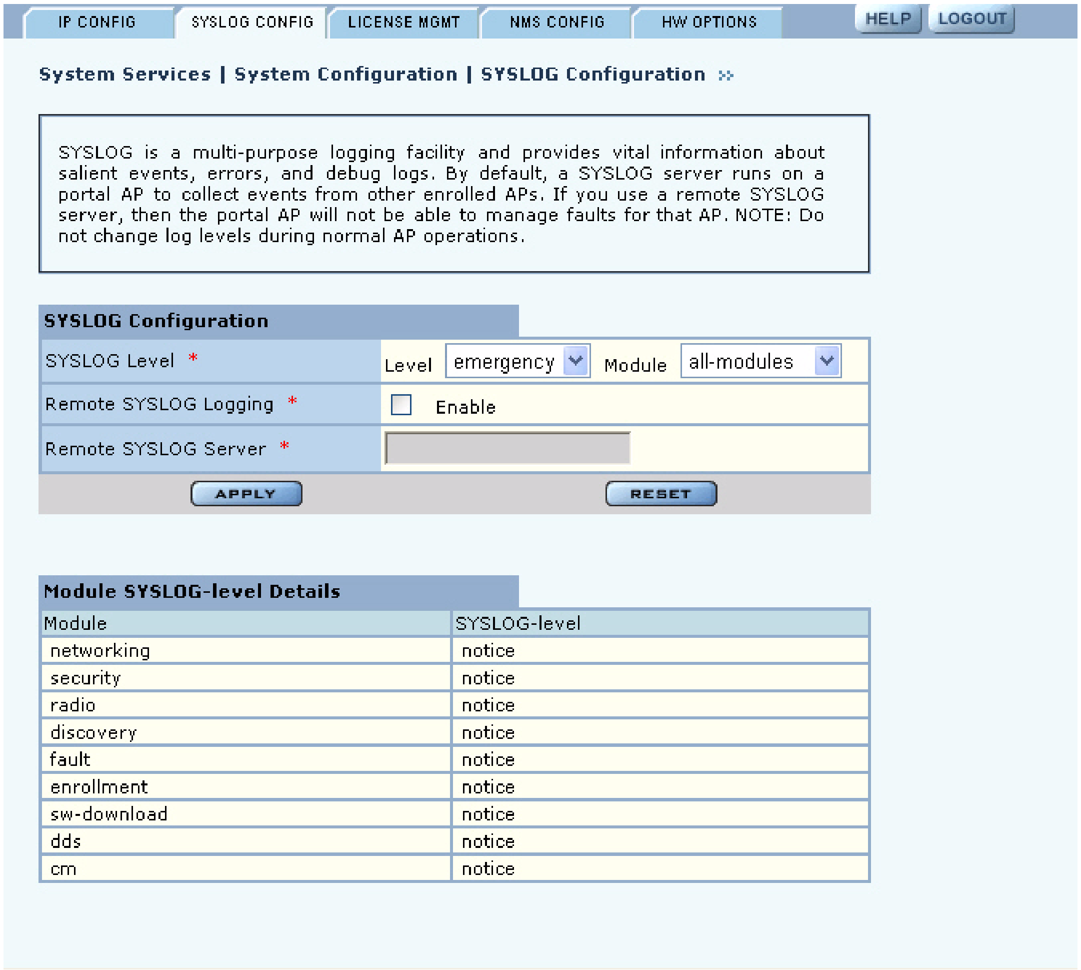
Syslog Configuration

Syslog tracks and records information about network activities for later viewing and analysis.

! **CAUTION:** Only an authorized administrator should change syslog levels or enable or disable syslog capabilities. Arbitrary changes to syslog can adversely affect the AP.

The top area of the Syslog panel (Figure 159) provides controls to set the logging level and scope for a variety of functional areas or modules.

Figure 159: System Configuration - Syslog Configuration



System Services | System Configuration | SYSLOG Configuration »

SYSLOG is a multi-purpose logging facility and provides vital information about salient events, errors, and debug logs. By default, a SYSLOG server runs on a portal AP to collect events from other enrolled APs. If you use a remote SYSLOG server, then the portal AP will not be able to manage faults for that AP. NOTE: Do not change log levels during normal AP operations.

SYSLOG Configuration

SYSLOG Level *	Level emergency Module all-modules
Remote SYSLOG Logging *	□ Enable
Remote SYSLOG Server *	

Module SYSLOG-level Details

Module	SYSLOG-level
networking	notice
security	notice
radio	notice
discovery	notice
fault	notice
enrollment	notice
sw-download	notice
dds	notice
cm	notice

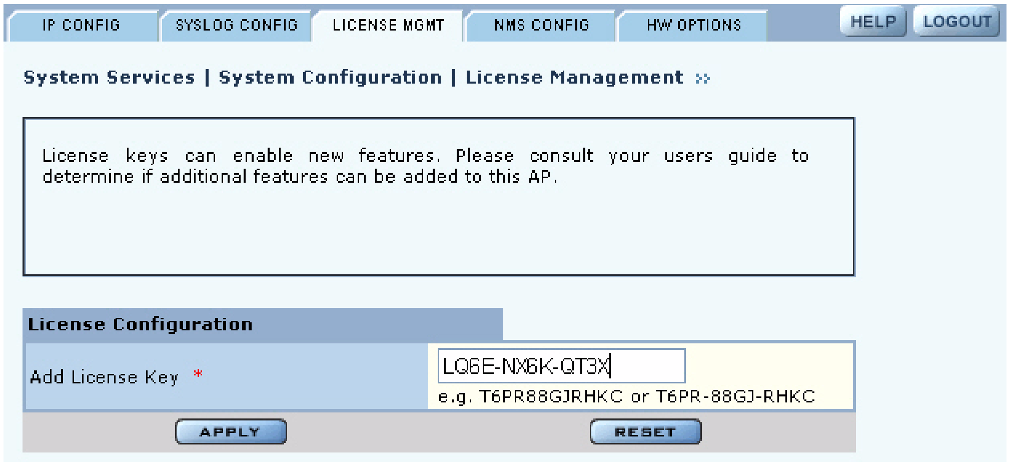
The tab contains the following settings:

Field	Description
Syslog-Level	Select the activity level that triggers a syslog entry. Choose from several levels (Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug). (required)
Syslog-Level Module	Select whether to record a specific type of activity, or include all the activities in the list. (required)
Remote Syslog Logging	Indicate whether to enable a remote server to monitor events across the network.
Remote Syslog Server	If the Syslog server is enabled, enter the remote server hostname or IP address.
Remote Syslog Server Port	If the Syslog server is enabled, enter the IP address or hostname of the server port. (optional)

License Management

Use the License Management tab (Figure 160) if it is necessary to change the license key for the AP. Enter or verify the license key for the AP, and click Apply. Click **Reset** to restore the previous license key.

Figure 160: System Configuration - License Management



System Services | System Configuration | License Management

License keys can enable new features. Please consult your users guide to determine if additional features can be added to this AP.

License Configuration

Add License Key * LQ6E-NX6K-QT3X

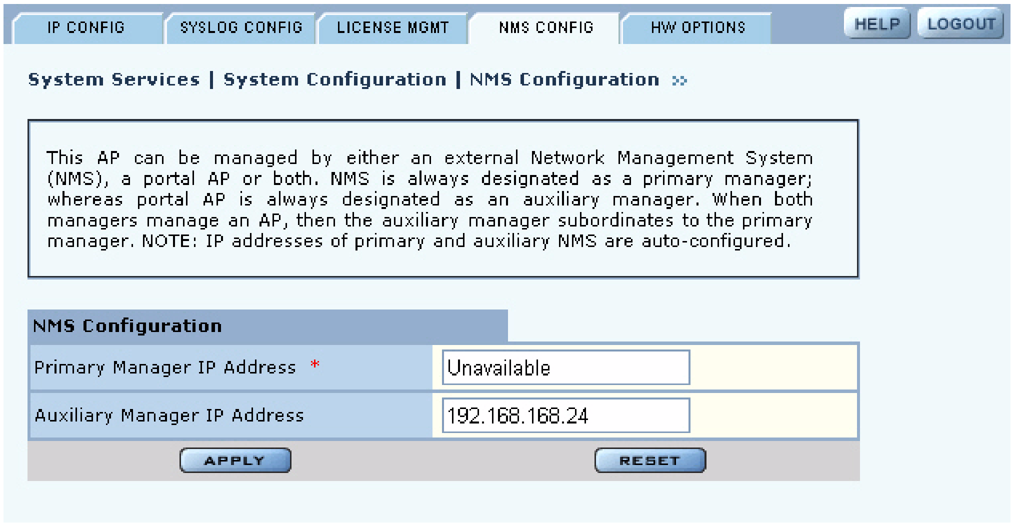
e.g. T6PR88GJRHKC or T6PR-88GJ-RHKC

NMS Configuration

Use the NMS Configuration tab (Figure 161) to identify network management servers and to determine which network management system will receive fault and event notifications.

NOTE: If the AP is already enrolled, it is not necessary to modify the settings on this panel.

Figure 161: System Configuration - NMS Configuration



This AP can be managed by either an external Network Management System (NMS), a portal AP or both. NMS is always designated as a primary manager; whereas portal AP is always designated as an auxiliary manager. When both managers manage an AP, then the auxiliary manager subordinates to the primary manager. NOTE: IP addresses of primary and auxiliary NMS are auto-configured.

NMS Configuration

Primary Manager IP Address *	Unavailable
Auxiliary Manager IP Address	192.168.168.24

Enter the following values to set the NMS configuration:

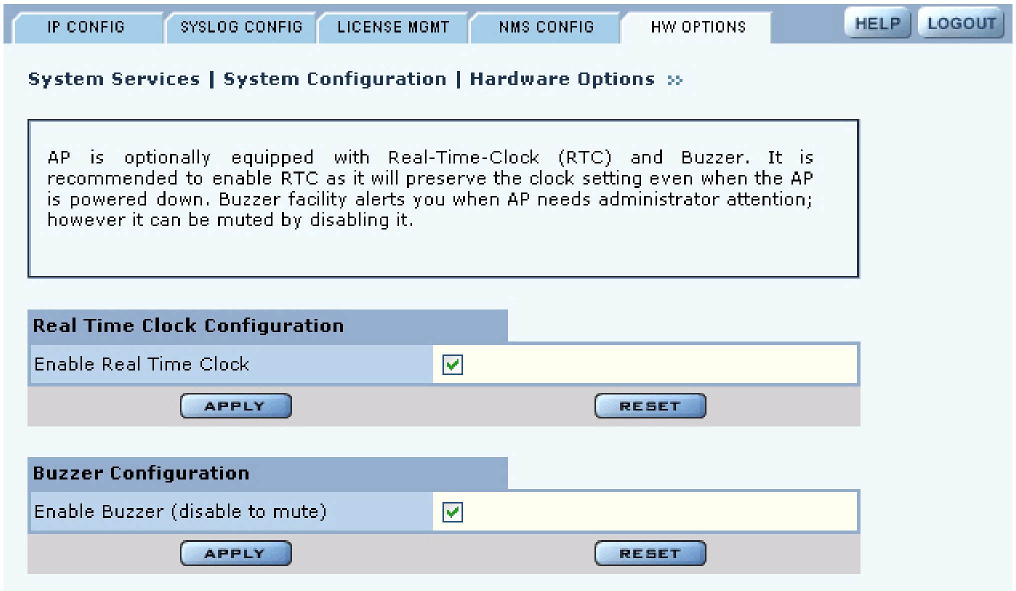
Field	Description
Primary Manager IP	Enter the IP address of the NM Portal or Wireless LAN Network Management Software server responsible for managing the AP. (required)
Auxiliary Manager IP	If applicable, enter the IP address of the NM Portal AP used to manage the AP at the branch location (in conjunction with an Wireless LAN Network Management Software server as a primary manager.

Click **Apply** to save the entries or **Reset** to return to the previously saved values.

Hardware Options

Select **HW Options** (Figure 162) to set the buzzer and the real time clock (RTC), which keeps track of the date and time in the event that the AP loses power. This feature is not required if the AP is always connected to the Internet.

Figure 162: System Configuration - Hardware Options



AP is optionally equipped with Real-Time-Clock (RTC) and Buzzer. It is recommended to enable RTC as it will preserve the clock setting even when the AP is powered down. Buzzer facility alerts you when AP needs administrator attention; however it can be muted by disabling it.

Real Time Clock Configuration

Enable Real Time Clock ☑

Buzzer Configuration

Enable Buzzer (disable to mute) ☑

Select the following parameters on this tab

Field	Description
Enable Real Time Clock	Use the real time clock (RTC).
Enable Buzzer	Activate the AP buzzer to locate the AP, if necessary.

Click **Apply** to save the entries or **Reset** to return to the previously saved values.

Managing the AP Configuration

Choose **Configuration Management** from the System Services menu to open the Configuration Management feature panel. The panel contains the following tabs:

- Secure Backup—Use https to perform a secure backup of the AP configuration.
- Configuration Backup—Back up and restore configurations, export log files, and reset the AP configuration to the factory defaults.
- Configuration Reports—View configuration reports for the AP.
- Reset Configuration—Revert to the factory default configuration, or reset specify subsystems to default configuration.

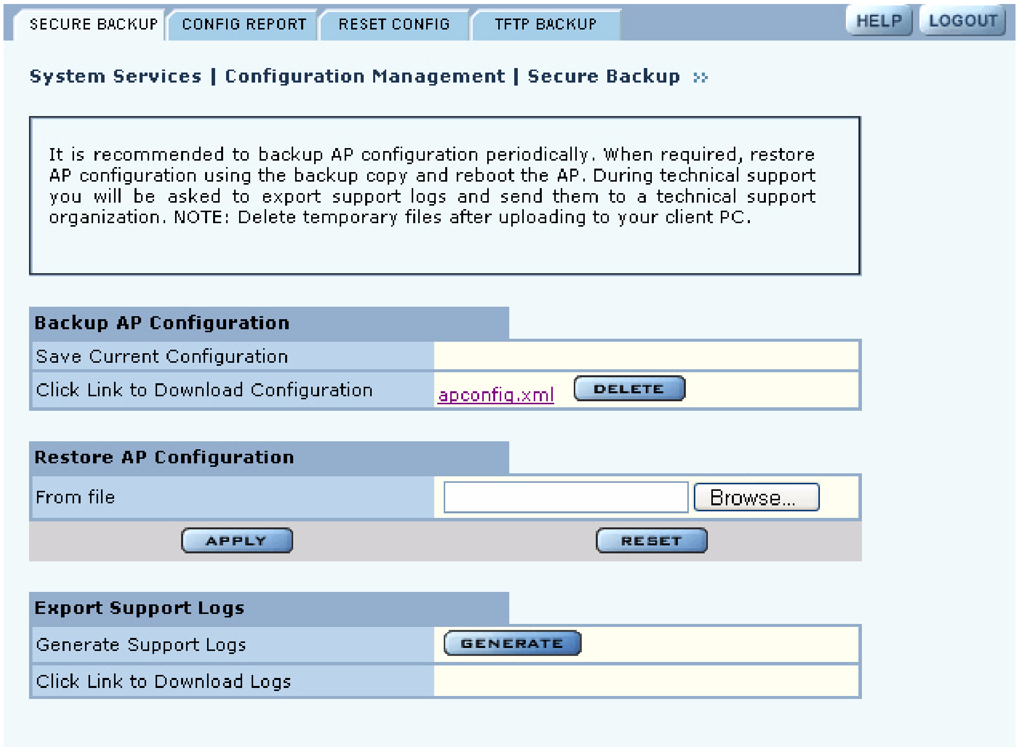
Secure Backup

Perform the following functions on the Secure Backup tab (Figure 166):

Task	Steps
Back up the AP configuration using https	1 Click **Save Configuration**. 2 When the configuration is generated, a hyperlink is displayed. Right-click and select **Save As** to save the configuration locally. 3 After the configuration file is saved, click **Delete** to remove the file from the AP. The file takes up space on the AP disk, so it is recommended to remove it.

Task	Steps
Restore the AP configuration	1 In the Restore Configuration area, click **Browse** and select the configuration file. 2 Click **Apply** to restore the configuration and reboot the AP. **NOTE:** If the AP has been unenrolled or restored to factory defaults, it is not possible to reapply the configuration using this method. The AP must be reenrolled and have a new configuration created.
Generate support logs	1 Click **Generate Support Logs**. 2 When the configuration is generated, a hyperlink is displayed. Right-click and select **Save As** to save the configuration locally. 3 After the support logs file is saved, click **Delete** to remove the file from the AP. The file takes up space on the AP disk, so it is recommended to remove it.

Figure 163: Configuration Management - Secure Backup



System Services | Configuration Management | Secure Backup »

It is recommended to backup AP configuration periodically. When required, restore AP configuration using the backup copy and reboot the AP. During technical support you will be asked to export support logs and send them to a technical support organization. NOTE: Delete temporary files after uploading to your client PC.

Backup AP Configuration	
Save Current Configuration	
Click Link to Download Configuration	apconfig.xml DELETE

Restore AP Configuration	
From file	Browse...

Export Support Logs	
Generate Support Logs	GENERATE
Click Link to Download Logs	

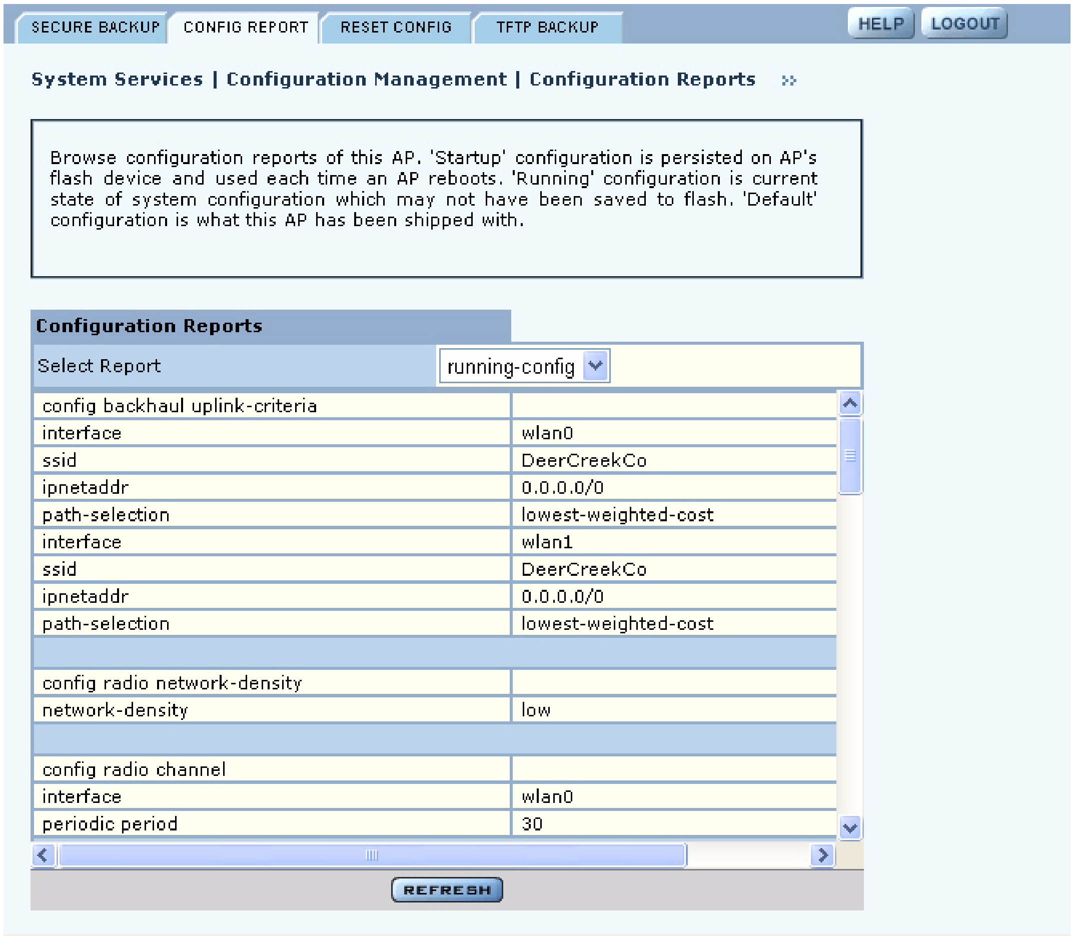
Configuration Reports

Select any of the following configuration reports on this tab (Figure 164):

Report	Description
Startup-Config	Provides details on the configuration that is stored on the AP flash device and used each time the AP reboots.
Running-Config	Provides details on the current AP configuration, which may or may not match the startup configuration.
Default-Config	Lists the factory default settings shipped on the AP.

Click **Refresh** to update the selected report

Figure 164: Configuration Management - Configuration Reports



SECURE BACKUP
CONFIG REPORT
RESET CONFIG
TFTP BACKUP
HELP
LOGOUT
System Services | Configuration Management | Configuration Reports

Browse configuration reports of this AP. 'Startup' configuration is persisted on AP's flash device and used each time an AP reboots. 'Running' configuration is current state of system configuration which may not have been saved to flash. 'Default' configuration is what this AP has been shipped with.

Configuration Reports

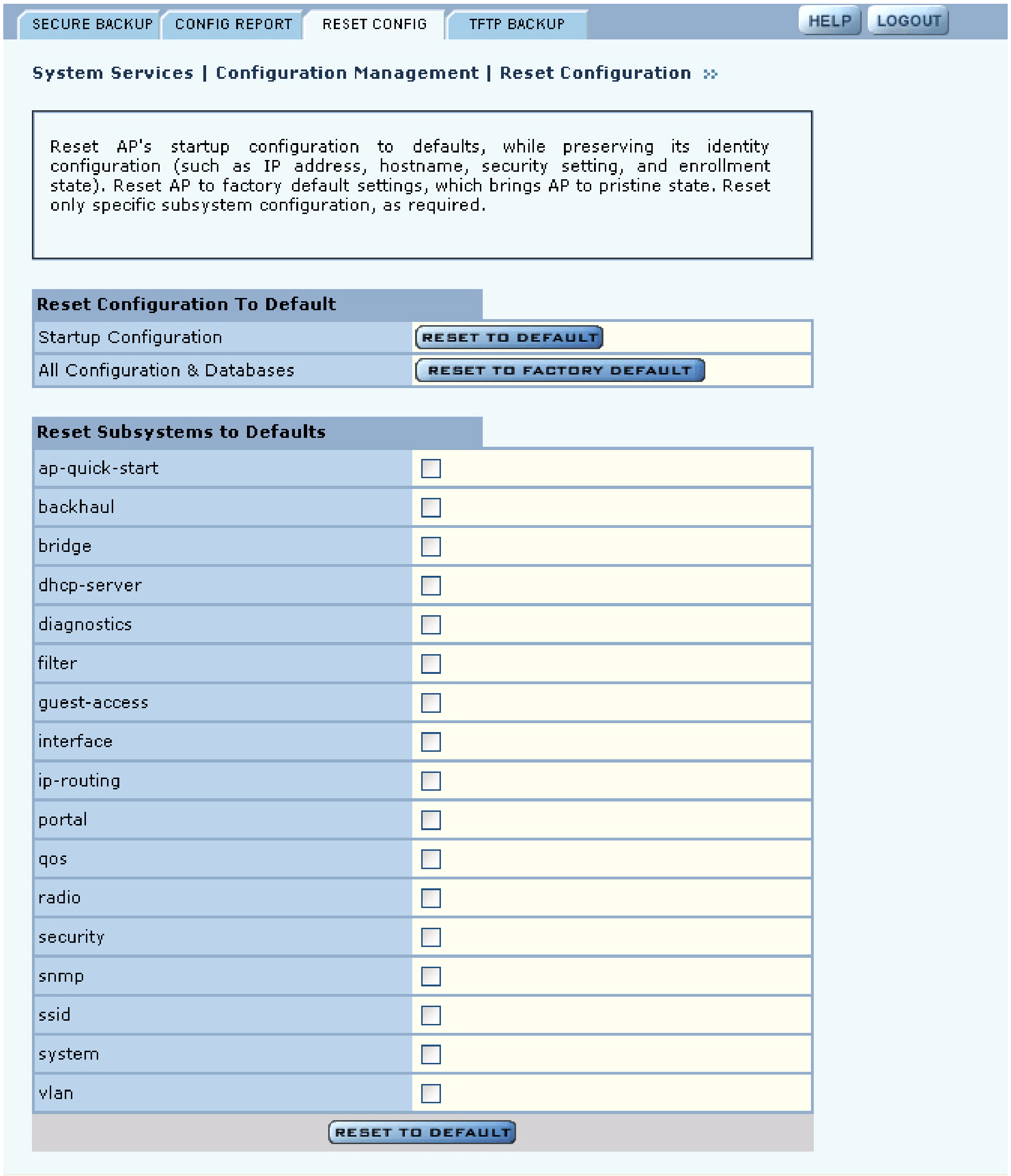
Select Report: running-config

config backhaul uplink-criteria	
interface	wlan0
ssid	DeerCreekCo
ipnetaddr	0.0.0.0/0
path-selection	lowest-weighted-cost
interface	wlan1
ssid	DeerCreekCo
ipnetaddr	0.0.0.0/0
path-selection	lowest-weighted-cost
config radio network-density	
network-density	low
config radio channel	
interface	wlan0
periodic period	30

Reset Configuration

Use the Reset Configuration tab to reset the AP configuration or revert to the defaults for individual subsystems (Figure 165).

Figure 165: Configuration Management - Reset Configuration



System Services | Configuration Management | Reset Configuration »

Reset AP's startup configuration to defaults, while preserving its identity configuration (such as IP address, hostname, security setting, and enrollment state). Reset AP to factory default settings, which brings AP to pristine state. Reset only specific subsystem configuration, as required.

Reset Configuration To Default	
Startup Configuration	RESET TO DEFAULT
All Configuration & Databases	RESET TO FACTORY DEFAULT

Reset Subsystems to Defaults	
ap-quick-start	□
backhaul	□
bridge	□
dhcp-server	□
diagnostics	□
filter	□
guest-access	□
interface	□
ip-routing	□
portal	□
qos	□
radio	□
security	□
snmp	□
ssid	□
system	□
vlan	□

Perform the following functions on this tab:

Function	Description
Reset to Default	**1** Select **Reset AP Startup Configuration Only** or **AP Configuration and Databases to Factory Defaults**. **2** Click **Apply** to reboot the AP with the selected configuration.
Reset Subsystems to Defaults	**1** Select one or more individual subsystems to reset. **2** Click **Apply** to reboot the AP with the selected defaults.

Click **Reset** to clear the selections on the tab.

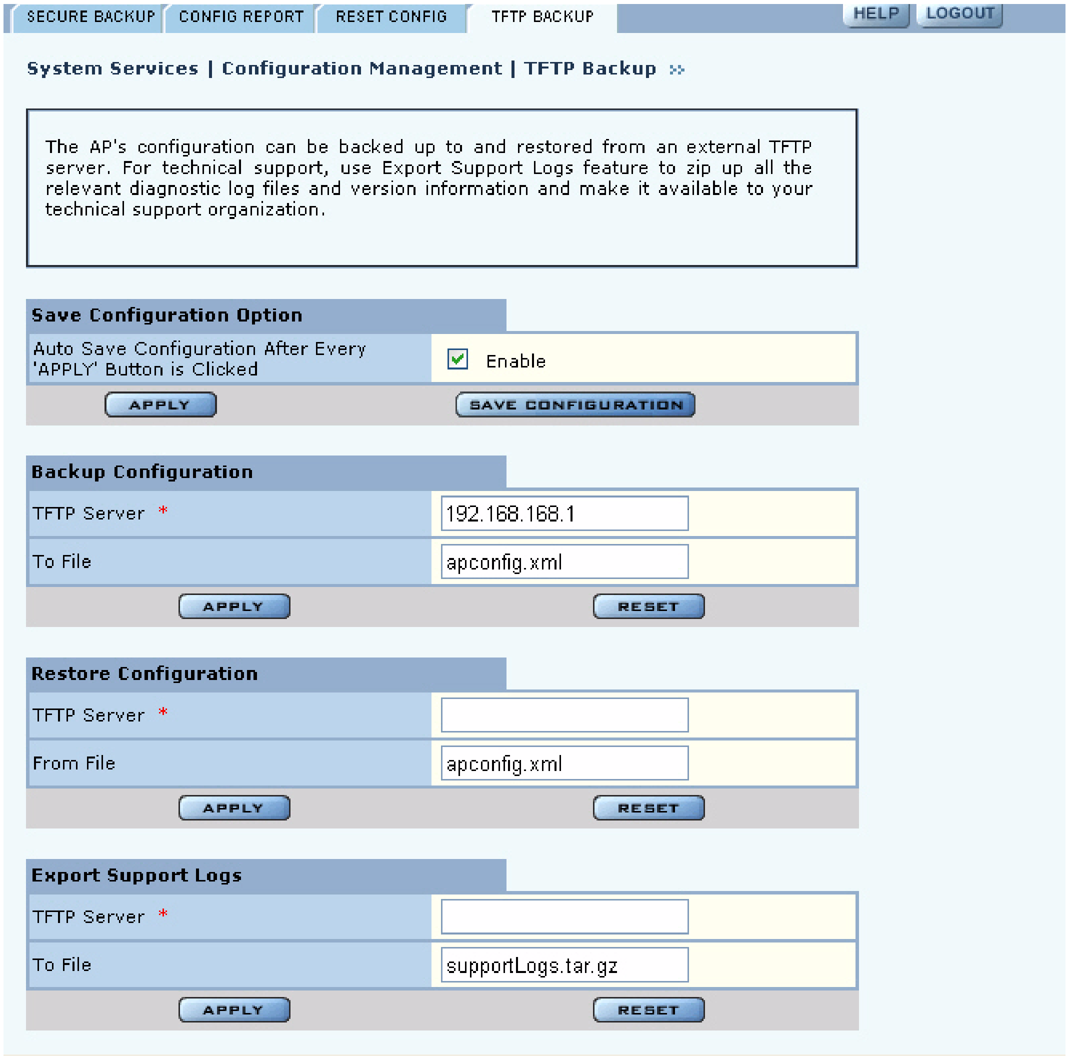
TFTP Backup

Use the TFTP Backup tab (Figure 166) to back up and restore configurations on an external TFTP server. Perform the following functions on this tab:

Task	Steps
Save configuration	**1** Indicate whether to save the AP configuration each time a save operation is done. **2** Click **Apply**. Click **Save Configuration** to save the current settings on demand.
Back up the configuration to a TFTP server	**1** Enter the IP address of the TFTP server. **2** Enter or confirm the configuration file name. **3** Click **Apply** to restore the configuration and reboot the AP. **NOTE:** If the AP has been restored to factory defaults, it is not possible to reapply the configuration using this method. The AP must be reenrolled and a new configuration created.
Restore the configuration	**1** Enter the IP address of the TFTP server. **2** Enter or confirm the name of the configuration file. **3** Click **Apply**.
Export support logs	**1** Enter the IP address of the TFTP server. **2** Enter or confirm the name of the log file. **3** Click **Apply**.

The Reset buttons on the panel clear the field entries in the associated section.

Figure 166: Configuration Management - TFTP Backup



System Services | Configuration Management | TFTP Backup

The AP's configuration can be backed up to and restored from an external TFTP server. For technical support, use Export Support Logs feature to zip up all the relevant diagnostic log files and version information and make it available to your technical support organization.

Save Configuration Option

Auto Save Configuration After Every 'APPLY' Button is Clicked: ☑ Enable

Backup Configuration

TFTP Server *	192.168.168.1
To File	apconfig.xml

Restore Configuration

TFTP Server *	
From File	apconfig.xml

Export Support Logs

TFTP Server *	
To File	supportLogs.tar.gz

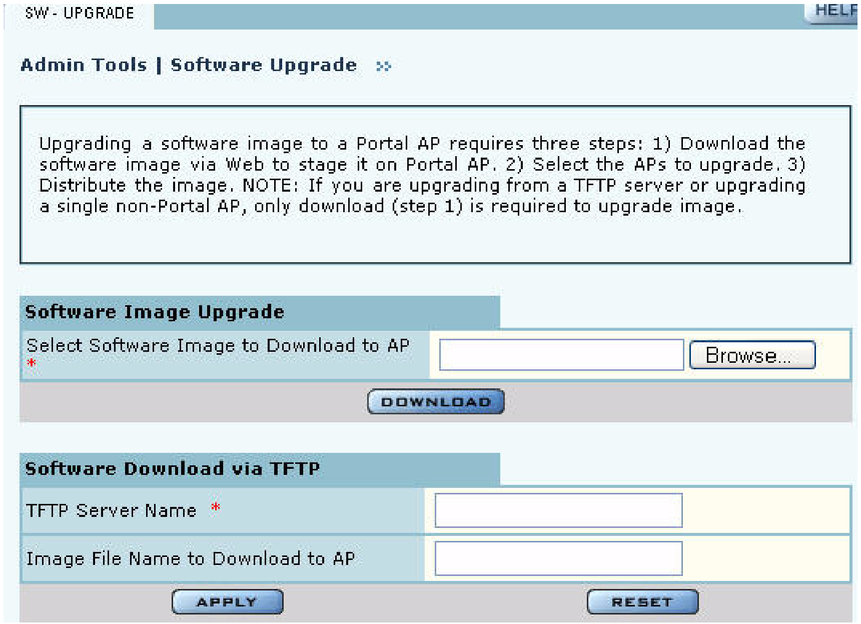
Upgrading Software

From the NM Portal web interface, you can upgrade the software on enrolled APs throughout the network in one operation. You can also upgrade any individual, non-portal AP from the AP web interface. The same interface is used for both situations; however, access to the interface is different for an NM Portal than for a non-portal AP.

- If the AP is an NM Portal, click **Manage Wireless Network** to open the NM Portal interface, and then choose **Admin Tools > Software Upgrade** to open the Software Upgrade panel (Figure 167).
- If the AP is a non-portal AP, choose **Admin Tools > Software Upgrade** to open the Software Upgrade panel.

NOTE: The AP license file is not affected by software upgrades. The existing software license remains valid after the AP software is upgraded.

Figure 167: Software Upgrade



SW - UPGRADE
HELP
Admin Tools | Software Upgrade »

Upgrading a software image to a Portal AP requires three steps: 1) Download the software image via Web to stage it on Portal AP. 2) Select the APs to upgrade. 3) Distribute the image. NOTE: If you are upgrading from a TFTP server or upgrading a single non-Portal AP, only download (step 1) is required to upgrade image.

Software Image Upgrade
Select Software Image to Download to AP *
Browse...
DOWNLOAD
Software Download via TFTP
TFTP Server Name *
Image File Name to Download to AP
APPLY
RESET

The Software Upgrade panel offers two upgrade options. The Software Image Upgrade option uses https to download the software image to the AP. The Software Download via TFTP option uses TFTP to download the software image. Select only one of these options; it is not possible to use both methods at the same time.

The software upgrade process for an NM Portal consists of the following three steps:

Step	Description
Staging	The software image is downloaded to the 108 Mbps Wireless AP.
Selection	APs are selected for software upgrade.
Distribution	The software upgrade image is distributed to the selected APs, installed, and the AP is rebooted.

If you are upgrading a non-portal AP or using TFTP as the download method, then the staging, selection, and distribution steps happen as a single process that cannot be interrupted once it begins. If you use the Software Image Upgrade selection in NM Portal, then staging, selection, and distribution are separate steps that can be monitored and canceled if needed.

Software Image File

The AP software image file conforms to an PLANEX-defined format that uses the filename extension `.img`. During download, the filename extension and structure are verified and the download is stopped if a problem with the file is detected.

Upgrading the AP Software

This section provides information for upgrading AP software using both the TFTP and https software download options.

i **NOTE:** It is important to perform software upgrades during a scheduled maintenance window. Upgrading takes approximately 4-5 minutes per AP, and upgrading multiple APs from an NM Portal is a serial process. To manage system resources during a software upgrade, the AP shuts down some services (such as CLI sessions) to create temporary memory and to validate the image prior to writing to AP's flash.

! **CAUTION:** Do not leave the Software Upgrade panel while download is taking place. Clicking on another menu item during download, the download process is canceled.

Upgrade Using https Download - Individual Non-Portal AP

To upgrade a non-portal AP using https download:

1. Choose **Admin Tools** > **Software Upgrade**.
2. Browse to select the `.img` software image file.
3. Click **Download**.
   A confirmation dialog appears asking you to confirm the software download.
4. Click **OK**.

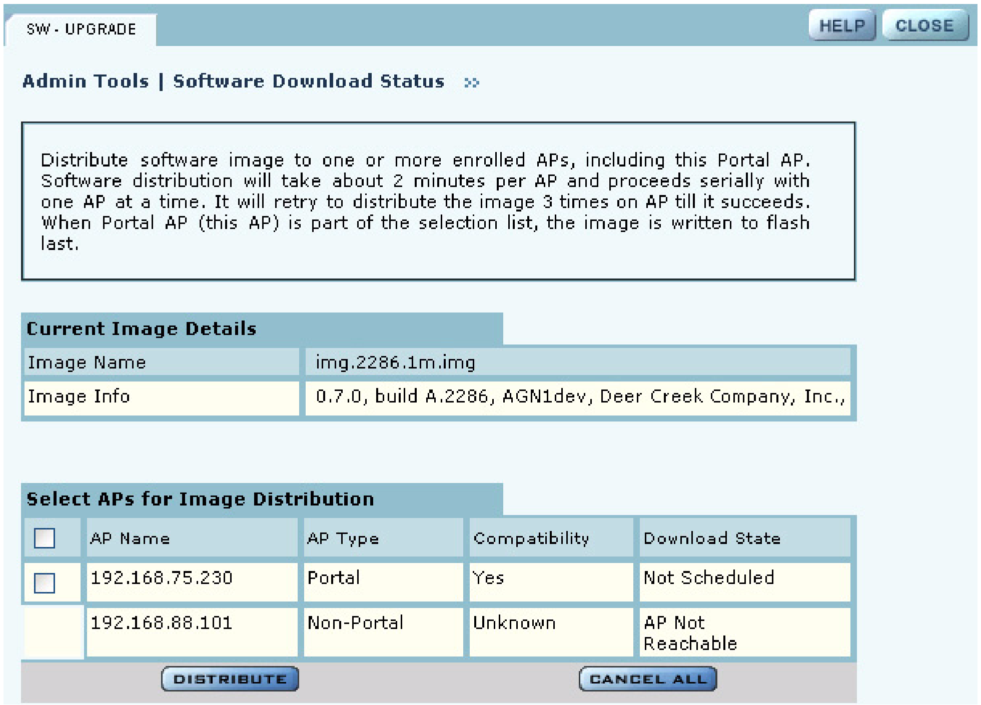
The software image is downloaded to the AP, the AP software image is upgraded, and the AP is automatically rebooted.

Upgrade and Distribution Using https Download - NM Portal AP

To upgrade APs from NM Portal using https download:

1. Choose **Admin Tools** > **Software Upgrade**.
2. Browse to select the `.img` software image file.
3. Click **Download**.
   A confirmation dialog asks you to confirm the software download.
4. Click **OK**.
   The system verifies the filename extension and header information. When successful, the Software Download Status panel opens (Figure 168). Staging is now complete.
5. Select the APs to receive the upgrade.
6. Click **Distribute**.
   A confirmation dialog asks you to confirm that the upgrade should now begin.
7. Click **OK**.

Figure 168: Software Upgrade - Download Status



Distribute software image to one or more enrolled APs, including this Portal AP. Software distribution will take about 2 minutes per AP and proceeds serially with one AP at a time. It will retry to distribute the image 3 times on AP till it succeeds. When Portal AP (this AP) is part of the selection list, the image is written to flash last.

Current Image Details

Image Name	img.2286.1m.img
Image Info	0.7.0, build A.2286, AGN1dev, Deer Creek Company, Inc.,

Select APs for Image Distribution

□	AP Name	AP Type	Compatibility	Download State
□	192.168.75.230	Portal	Yes	Not Scheduled
	192.168.88.101	Non-Portal	Unknown	AP Not Reachable

The software distribution process begins by sending the software to the first selected AP. As soon as this AP receives the software, it upgrades its image and reboots automatically. The process then moves to the next selected AP. After all the APs have been upgraded, the NM Portal AP is upgraded and rebooted. The administrator must again log in to the NM Portal web interface after an upgrade and reboot.

Upgrade Using TFTP Download

To upgrade an NM Portal or non-portal AP using TFTP download:

1. Choose **Software Upgrade** from the Admin Tools menu.
2. Enter the IP address of the TFTP server.
3. Enter the name of the image file on the TFTP server. The default file is `target.ppc.ani.img`, under the boot directory of the TFTP server. Relative paths can be used when specifying the file name.
4. Click **Apply**.

   A pop-up message asks for confirmation that you want the upgrade to begin.
5. Click **OK**.

   The download process begins. Every 10 seconds the screen is updated with new status information. If the download is successful, the AP is automatically rebooted with the new software image. If the download is unsuccessful, an explanatory message is displayed in the Download Status column.

Canceling a Distribution

To cancel software distribution at any time, you must click **Cancel All.** This cancels distribution to APs that have not yet been upgraded, restarts services that were shut down during the upgrade, and removes the image file from the AP RAM. Cancellation is performed serially for multiple AP distributions. Canceling during distribution does not cause any damage to the APs. If the distribution on a remote AP is cancelled, the AP will be automatically rebooted. You can cancel distribution to an individual AP at any time except when the status is Updating Flash…, Error, or Done (Rebooting…).

If you leave the Software Upgrade panel before the distribution is complete without clicking the **Cancel All**, software distribution continues in the background, but it is not possible to return to the Distribution Status page.

Download Status

During distribution, the Download State column displays the current status of the distribution process (see Figure 168).

Status information is automatically updated every 10 seconds. The status information shows clearly the stage of the distribution process and identifies any problems. Table 15 lists the possible status values and their meaning.

Status	**Explanation**
Not scheduled	This AP has not been scheduled to receive a software update.
Scheduled	The update has been ordered for this AP, but has not yet begun.
Canceling	A request has been made to cancel the distribution; however, the request is not complete. For example, this message is displayed if a request has been made to cancel distribution to an AP waiting its turn in the distribution list.
Canceled	Distribution to the AP is canceled.
AP Unreachable	The enrolled AP is not reachable for distribution.
Retrying 1, Retrying 2	If communication with the AP is lost during distribution, the process waits for two minutes and then retries the distribution. Three retries are attempted before the process stops and an error message is presented. Retrying 1 and Retrying 2 status represent the first and second retries. Retries may occur, for example, during upgrade of backhaul APs, if the radio signal is temporarily lost and retrunking is required. There is a timeout of 2 minutes in between retries. With a total of three retries, it can take up to 10 minutes before a distribution on an AP is deemed to be in error. The message changes to In Progress .. (XX %) when the retry actually starts.
In Progress .. (XX %)	Upgrade is underway on the AP and is XX% complete.
Error	All retries have finished and the AP could not be upgraded due to some internal error.
Unknown	An unknown error has occurred.
Image Integrity Error	The image has passed the compatibility test but failed the integrity check after the distribution, but before the flash update.
Updating Flashing ...	Image distribution is complete and it is being saved onto the AP's flash memory.

Status	Explanation
Done. Rebooting...	The flashing is complete and the AP is rebooting.

When the distribution is complete, the message Software Distribution is Complete is displayed, regardless of whether the distribution was successful. If a portal AP is not included in the download, then all services restarted automatically after the distribution.

Image Recovery

During the upgrade process, care is taken to validate the image integrity and compatibility with AP hardware. If a new image is successfully upgraded but fails to initialize during subsequent reboot, AP automatically performs a "safe" boot from the backup partition.

Common Problems and Solutions

Table 15 lists common problems that can occur along with recommended solutions.

Table 15: Common Problems and Solutions

Symptom	Problem	Solution
AP power and Ethernet Link LEDs are off.	Power is off or unconnected.	Check the power connection to make sure it is plugged in. Also check the power outlet. If necessary, plug some other appliance into the outlet to verify power.
AP power LED is on, but the Ethernet Link LED is off.	Ethernet cable is unconnected or unable to access the LAN.	Check the Ethernet cable connection between the AP and network port. Make sure to use a regular CAT-5 standard Ethernet cable, and not a crossover cable (usually used for uplinks between switches and routers). If in doubt, swap the cable for a known, working cable. If the port is non-functional, it may be necessary to use another working network port.
Unable to configure the Access Point through the web browser interface.	Computer is unable to reach the Access Point over the Local Area Network (LAN).	Check to make sure the Access Point power LED is on. Check the Ethernet cable connections to both the computer and to the AP. Make sure that the network adapter in the computer is working properly. Check to see whether the IP address is on the same subnet as the Access Point.

Table 15: Common Problems and Solutions

Symptom	Problem	Solution
Poor or lower than expected signal strength, as measured by wireless network adapters attempting to connect to the Access Point.	Access Point may be poorly placed, or external antenna not connected properly.	The Access Point and/or its external antenna should not be in an obstructed location. Metallic objects (such as equipment racks) and some construction materials can block wireless signals. If this is the case, reposition the Access Point(s) and/or any external antennae to be free of these obstructions. If using an external antenna, also make sure that it is connected securely to the Access Point.

A Using the Command Line Interface

This appendix explains how to access and interact with the command line interface (CLI). For detailed information on specific commands, see the CLI Reference Manual.

Using the Command Line Interface

To connect to the AP for command line interface access using Secure Shell (SSH), do the following:

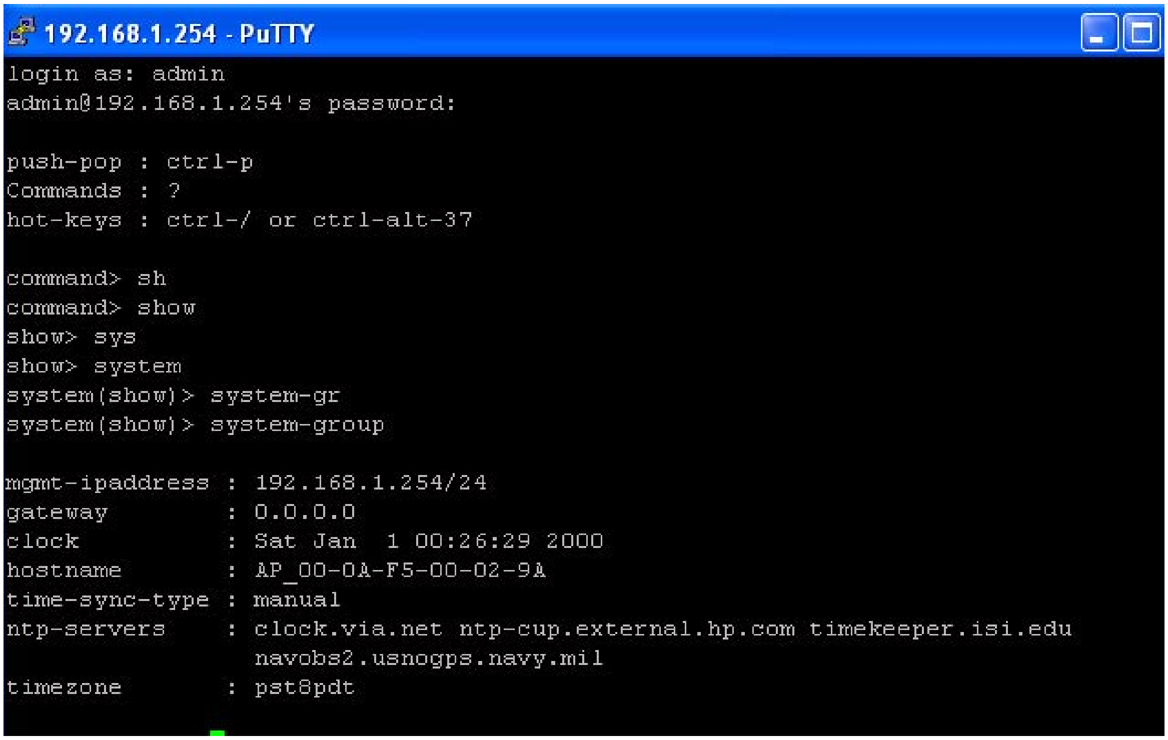
1 Launch your SSH client application.

NOTE: SSH Communications provides an SSH client, http://www.ssh.com.

2 Type `ssh admin@<AP IP address>`, using the AP IP address assigned to the Access Point (or `192.168.1.254` by default) and press Return.

When connected, a screen opens similar to the one shown in Figure 169.

Figure 169: Access Point Serial Console Login Screen



```
login as: admin
admin@192.168.1.254's password:

push-pop : ctrl-p
Commands : ?
hot-keys : ctrl-/ or ctrl-alt-37

command> sh
command> show
show> sys
show> system
system(show)> system-gr
system(show)> system-group

mgmt-ipaddress  : 192.168.1.254/24
gateway         : 0.0.0.0
clock           : Sat Jan  1 00:26:29 2000
hostname        : AP_00-0A-F5-00-02-9A
time-sync-type  : manual
ntp-servers     : clock.via.net ntp-cup.external.hp.com timekeeper.isi.edu
                  navobs2.usnogps.navy.mil
timezone        : pst8pdt
```

3 Enter your login ID and press Return. When prompted next, enter your password. The factory default for administrator access is user name: `admin`. If the AP has not been initialized, the user name field is grayed out. The factory default password is shipped with the AP on a paper insert. Use the password from the insert to log in.

4 To see the list of available commands, type a question mark (?). For a list of hot keys (short cuts for console functions, press Ctrl-H.

There are two important modes in console access, one is *show* mode and the other is *config* mode. In show mode, examine the AP's configuration settings and status. Use config mode to change values. To go into either mode from the main `command>` prompt, type either show or config.

Toggle between show and config modes by pressing Ctrl-P. Leave a mode and return to the top level command prompt by typing `exit`.

5 To log out and close your connection to the command line interface, type `logout` at any prompt.

Using the Console Port for CLI Access

To connect to the AP for command line interface (CLI) access using the built-in console port, do the following:

1 Connect your computer to the AP console port using a serial DCE cable (this is typically a 9-pin-to-9-pin cable with the transmit and receive lines crossed over a null modem cable). A USB-to-Serial adapter may be required if the computer lacks a 9-pin serial port.

2 Launch your terminal emulation application. On PCs running Microsoft Windows operating systems, the Microsoft-provided application HyperTerminal will work fine. (This is accessed usually through `Programs > Accessories > Communications > HyperTerminal`. The remainder of this procedure assumes the use of HyperTerminal. Modify the procedures accordingly if using another application.)

3 Create a terminal connection profile if one does not already exist. Enter a descriptive name and select any icon from the list provided. Click **OK** when done.

If there is a working HyperTerminal connection profile, select that shortcut instead to launch the connection, and skip to step 7.

4 The Connect To screen displays. The important element there is to use the `Connect using:` drop down box, and select the serial port to which the AP is connected. Click OK when done.

5 Use the following port settings:

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

6 Click OK when done. When connected, a screen opens similar to the one shown in Figure 169.

7 If the console login screen in the HyperTerminal does not open, press **Return** once or twice. If you still see nothing or garbage characters appears, check the cable connection and the terminal connection parameters.

8 Enter your login ID and press Return. When prompted next, enter your password. (The AP defaults are login `admin` and password: `password`, and login `opr` and password `opr` for operator (read-only) access.)

9 To see the list of available commands, type a question mark (?). For a list of hot keys (short cuts for console functions, press Ctrl-H.

There are two important modes in console access, one is *show* mode and the other is *config* mode. In show mode, examine the AP's configuration settings and status. Use config mode to change values. To go into either mode from the main `command>` prompt, type either show or config.

Toggle between show and config modes by pressing Ctrl-P. Leave a mode and return to the top level command prompt by typing `exit`.

To log out and close your connection to the command line interface, type `logout` at any prompt.

B Regulatory and License Information

This appendix contains the regulatory and license information specific to the 108 Mbps Wireless Access Point hardware and software.

Table 16: Regulatory and License Compliance

ID	Access Point Requirement	Details
CERT1	Safety	UL 1950 third edition
		TUV approval
		UL-2043 (Fire and Smoke) Compliance
CERT2	EMC	EMC Directive 89/336/EEC (CE Mark)
CERT3	Radio Approvals	FCC CFR47 Part 15, section 15.247
		FCC (47CFR) Part 15B, Class B Emissions
		Canada IC RSS210
		Japan MPT Radio Regulations
		Europe: ETS 300.328

C Alarms

Alarms generated by the 108 Mbps Wireless Access Point are stored persistently on the AP. The 108 Mbps Wireless AP can store approximately 130 * 2 = 260 alarms in total. When the number of alarms exceeds this limit, the oldest alarm set is discarded.

All alarms generated by the 108 Mbps Wireless Access Point have the following parameters:

- **Event ID**: The internal event number that uniquely identifies the event.
- **Log-level**: The criticality of the event. All alarms are logged at the same criticality.
- **Log-time**: The time as determined by the clock on the Access point, when the alarm was logged. All forwarded alarms have the log-time set to the clock time on the originating Access point.
- **Module**: The subsystem on the Access point that generated the alarm.
- **Source**: The hostname or IP address of the access point that generated the alarm.
- **Description**: The alarm details.

Use the 108 Mbps Wireless AP CLI to display the alarm table as follows:

Examples: `system(show)> alarm-table`

```
event-id    : 102
log-level   : 2
log-time    : Tue Jan  4 16:14:01 2000
module      : WSM
source-ip   : AP_00-0A-F5-00-02-1F
description : Device ID AP_00-0A-F5-00-02-1F radio 6 is enabled, its operational
              state is 2 operating on 11
-------------------------------------------------------------------------------
event-id    : 103
log-level   : 2
log-time    : Tue Jan  4 17:04:28 2000
module      : WSM
source-ip   : AP_00-0A-F5-00-02-1F
description : Device Id AP_00-0A-F5-00-02-1F radio 4 disabled
-------------------------------------------------------------------------------
```

The following section describes in detail the alarm syntax and alarm parameters. The alarm and its parameters together are shown as “description” above. The following alarms are described:

- “Discovery: Discovered new node” on page 237
- “Discovery: Node deleted from network” on page 237
- “Discovery: Managed nodes limit exceeded” on page 238
- “Enrollment: Node Enrolled” on page 238
- “Enrollment: Node Un-enrolled” on page 239
- “Policy: Policy Download Successful” on page 240

- “Policy: Policy Download Failed” on page 240
- “Software Download: Image Download Succeeded” on page 241
- “Software Download: Image Download Failed” on page 241
- “Software Download: Software Distribution Succeeded” on page 242
- “Wireless: Radio enabled (BSS Enabled)” on page 243
- “Wireless: Radio Disabled (BSS disabled)” on page 243
- “Wireless: BSS Enabling Failed” on page 244
- “Wireless: Frequency Changed” on page 244
- “Wireless: STA Association Failed” on page 245
- “Wireless: STA Associated” on page 246
- “Wireless: STA Disassociated” on page 247
- “Wireless: WDS Failed” on page 248
- “Wireless: WDS Up” on page 249
- “Wireless: WDS Down” on page 249
- “Security: Guest Authentication Succeeded” on page 250
- “Security: Guest Authentication Failed” on page 251
- “Security: User rejected by RADIUS Server” on page 252
- “Security: BP rejected by RADIUS Server” on page 252
- “Security: RADIUS Server timeout” on page 253
- “Security: Management User login success” on page 254
- “Security: Management User login failure” on page 255
- “Security: STA failed EAPOL MIC check” on page 255
- “Security: STA attempting WPA PSK – no Pre-shared Key is set for SSID” on page 256
- “Security: Auth Server Improperly configured on this SSID” on page 257
- “Security: STA failed to send EAPOL-Start” on page 258
- “Security: RADIUS sent a bad response” on page 259
- “Security: RADIUS timeout too short” on page 259
- “Security: STA authentication did not complete in time” on page 260
- “Security: Upstream AP is using an untrusted auth server” on page 261
- “Security: Upstream AP failed MIC check during BP authentication” on page 263
- “Security: Premature EAP-Success received” on page 263
- “Security: Profile not configured for user-group” on page 264
- “Security: STA has failed security enforcement check” on page 265
- “Security: Guest Authentication Failed” on page 267
- “Security: BP Detected Bad TKIP MIC on Incoming Unicast” on page 269
- “Security: BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast” on page 269
- “Security: STA Detected Bad TKIP MIC on Incoming Unicast” on page 270
- “Security: STA Detected Bad TKIP MIC on Incoming Multicast/Broadcast” on page 271
- “Security: TKIP counter-measures lockout period started” on page 271
- “Security: EAP response timeout” on page 273
- “Security: EAPOL Key exchange – message 2 timeout” on page 274
- “Security: EAPOL Group 2 key exchange timeout” on page 275

Discovery: Discovered new node

Alarm generated when a new 108 Mbps Wireless AP is discovered in the nework.

Syntax: `DeviceId %s discovered node [deviceId=%s, IP=%s, Subnet=%s].`

Alarm Parameters

DeviceID	The Portal's Device ID.
deviceId	The discovered node's device ID
IP	The discovered node's IP address
Subnet	The Subnet to which the discovered node belongs

Alarm Severity

Severity	Critical

Description: This alarm is generated when an 108 Mbps Wireless AP is discovered by the NM Portal the first time.

Usage: Informational log.

Examples:

```
DeviceId AP_00-0A-F5-00-02-1F discovered node [deviceId=AP_00-0A-
F5-00-01-B0, IP=192.168.75.244, Subnet=255.255.254.0].
```

See Also: `<Node deleted from network>`

Discovery: Node deleted from network

Generated when a node is deleted from the Portal network.

Syntax: `DeviceId %s Node [Ip=%s, persona=%d] deleted from database.`

Alarm Parameters

DeviceId	The Device ID of the NM Portal
Ip	The IP address of the node being deleted.
Persona	The Persona of the node being deleted.

Alarm Severity

Severity	Critical

Description: This alarm is generated when the a discovered node is deleted from the system. When a node is deleted, all information about that node is erased from the Portal. If the node's IP address falls within the discovery scope, then the node will be re-discovered and added back to the set of the discovered nodes on the next discovery sweep.

Usage: Informational log.

Examples:

```
DeviceId AP_00-0A-F5-00-02-1F Node [Ip=192.168.74.210, persona=6]
deleted from database.
```

See Also: `<Discovered new node>`

Discovery: Managed nodes limit exceeded

Generated when a the number of nodes discovered exceeds the predefined limit on the NM portal.

Syntax:

```
On Device %s Node[Ip=%s] managed node limit exceeded. Current
managed nodes limit is %d.
```

Alarm Parameters

Device	The Device ID of the NM Portal
IP	The IP address of the node being deleted.
Node Limit	The current limit imposed on the discovery server.

Alarm Severity

Severity	Critical

Description: This alarm is generated when the number of discovered nodes exceeds the predefined limit. The current limit on number of access points discovered is 50. This limit can be configured to be lower.

Usage: If this alarm occurs then the discovery server will not discover nor track any new nodes once this limit is reached. In such case, delete unwanted nodes and manually add the nodes to the discovery database so that they may be managed.

Examples:

```
On Device AP_00-0A-F5-00-02-1F Node[Ip=192.168.74.245] managed node
limit exceeded. Current managed nodes limit is 10.
```

See Also:

Enrollment: Node Enrolled

Alarm generated when an 108 Mbps Wireless AP is enrolled into the nework

Syntax: NMPortal with **DeviceId** %s has successfully enrolled a remote node having **ApDeviceId**=%s **NodeIp**=%s and **Persona**=%d

Alarm Parameters

DeviceId	The Device ID of the NMPortal
ApDeviceId	The Device ID of the remote AP

NodeIp	The IP address of the remote AP
Persona	The Persona of the remote AP 6 = Security Portal 2 = Normal AP

Alarm Severity

Severity	Critical

Description: This alarm is generated when the 108 Mbps Wireless AP has been successfully enrolled into the network.

Usage: Informational log.

Examples:

```
NMPortal with DeviceId AP_00-0A-F5-00-01-77 has successfully enrolled a remote node
having DeviceIdId=AP_00-0A-F5-00-01-7A NodeIp=172.16.12.4 and persona=2
```

See Also: `<Node Unenrolled>`

Enrollment: Node Un-enrolled

Alarm generated when the 108 Mbps Wireless AP is rejected (un-enrolled) from the nework

Syntax: NMPortal with **DeviceId** %s has successfully unenrolled the remote node having **ApDeviceId**=%s **NodeIp**=%s and **Persona**=%d

Alarm Parameters

DeviceId	The Device ID of the NMPortal
ApDeviceId	The Device ID of the remote AP
NodeIp	The IP address of the remote AP
Persona	The Persona of the remote AP 6 = Security Portal 2 = Normal AP

Alarm Severity

Severity	Critical

Description: This alarm is generated when the 108 Mbps Wireless AP has bee successfully rejected (un-enrolled) from the network.

Usage: Informational log.

Examples:

```
NMPortal with DeviceId AP_00-0A-F5-00-01-77 has successfully enrolled a remote node
having DeviceIdId=AP_00-0A-F5-00-01-7A NodeIp=172.16.12.4 and persona=2
```

See Also: `<Node Enrolled>`

Policy: Policy Download Successful

Alarm generated when a policy is successfully downloaded to an AP.

Syntax: For accesspoint **Node** %s The **policy** [%s] **from** [%s] was successfully downloaded at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
policy	The policy name
from	The device ID of the source of the policy
time	The time at which the policy was consumed

Alarm Severity

Severity	Critical

Description: This alarm is generated when a policy is successfully downloaded to an AP.

Usage: Informational log.

Examples:

```
For accesspoint Node AP_00-0A-F5-00-01-77 The policy [security.xml]
from [TrustedManager] was successfully downloaded at time[Thu Jan 6
04:27:45 2000 ]
```

See Also: `<Policy Download Failed>`

Policy: Policy Download Failed

Alarm generated when a policy is download to an AP failed.

Syntax: For accesspoint **Node** %s the **policy** [%s] **from** [%s] could not be downloaded due to **error** %d at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
policy	The policy name
from	The device ID of the source of the policy
error	The failure error code
time	The time at which the policy was consumed

Alarm Severity

Severity	Critical

Description: This alarm is sent when a policy downloaded to an AP could not be consumed correctly either due to an error in the policy or software version mismatch or due to some other error.

Usage: Informational log.

Examples: For accesspoint Node AP_00-0A-F5-00-01-7D The policy [defaultpolicy.xml] from [TrustedManager] could not be downloaded due to error 22549 at time[Wed Feb 11 17:28:38 2004]

See Also: `<Policy Download Successful>`

Software Download: Image Download Succeeded

Alarm generated when an image is successfully downloaded and applied to an AP.

Syntax: For accesspoint **Node** %s the software **image** [%s] **from** [%s] was successfully downloaded at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
image	The image version information
from	The device ID of the source of the image
time	The time at which the image was consumed

Alarm Severity

Severity	Critical

Description: This alarm is when an image is successfully downloaded and applied to an AP.

Usage: Informational log.

Examples: For accesspoint Node AP_00-0A-F5-00-01-77 The software image [1.1.0, build 3278, AGN1dev, PLANEX Inc.,] from [AP_00-0A-F5-00-01-77] was successfully downloaded at time[Fri Jan 7 06:04:47 2000]

See Also: `<Image Download Failed, Software Distribution Succeeded>`

Software Download: Image Download Failed

Alarm generated when an image is un-successfully downloaded and applied to an AP.

Syntax: For accesspoint **Node** %s The software **image** [%s] **from** [%s] could not be downloaded due to **error** %d at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
image	The image version

from	The device ID of the source of the image
error	The failure error code
time	The time at which the error occurred

Alarm Severity

Severity	Critical

Description: This alarm is when an image is un-successfully downloaded and applied to an AP.
Usage: Image download failures can happen due to corrupted images, invalid length images or due to connectivity failures.
Examples: For accesspoint Node AP_00-0A-F5-00-01-77 The software image [] from [AP_00-0A-F5-00-01-77] could not be downloaded due to error 24581 at time[Fri Jan 7 04:12:35 2000]
See Also: `<Image Download Succeeded, Software Distribution Succeeded>`

Software Download: Software Distribution Succeeded

Alarm generated when an image distribution is completed.

Syntax: On **DeviceId** %s, the Software **image** [%s] distribution request from **portal**[%s] using the Distribution **TaskId**=%s and with **status**=%s completed at **time**[%s]

Alarm Parameters

DeviceId	The device ID of the remote AP
image	The image version
portal	The device ID of the source of the image (NMS or NMPortal)
TaskId	The task ID of the distribution
status	The distribution status (success or failure) of the selected APs
time	The time at which the distribution was done

Alarm Severity

Severity	Critical

Description: This alarm is when an image distribution is completed. Image distribution is
Usage: Informational log.
Examples: On DeviceId AP_00-0A-F5-00-01-77 , the Software image [0.7.0, build A.2286, AGN1dev, PLANEX Inc.,] distribution request from portal[AP_00-0A-F5-00-01-77] using the Distribution TaskId=000000 and with status=172.16.12.4, , 0, 947304168, 947304183, invalid image file. completed at time[Tue Jan 6 21:32:18 1970]
See Also: `<Image Download Failed, Image Download Succeeded>`

Wireless: Radio enabled (BSS Enabled)

Notification which indicates that AP radio has been enabled.

Syntax: "Device ID %s radio %d is enabled, its operational state is %d operating on %d"

Alarm Parameters	
DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
Operational Mode	This indicates the operational mode of the radio whether it is 802.11a, 802.11b or 802.11g
Channel ID	This indicates the channel on which the AP is operating.
Alarm Severity	
Severity	Critical

Description: Notification which is generated when a AP radio (BSS) is enabled

Usage: This indicates successful start of a BSS and also provides the channel on which the AP radio will be operating on.

Examples:

```
Device ID AP_00-0A-F5-00-01-B6 radio 4 is enabled, its operational mode is 1 and
operating on 64
```

See Also:

Wireless: Radio Disabled (BSS disabled)

Notification which indicates that the AP radio has been disabled.

Syntax: "Device Id %s radio %d disabled"

Alarm Parameters	
DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
Alarm Severity	
Severity	Critical

Description: Notification which indicates that AP has been disabled.

Usage: The AP radio can be disabled for several reasons such as:
a. User Triggered (administrative disabling)

b. Radio reset caused due to application of wireless specific configuration
c. Radio reset triggered by hardware
d. Radio reset due to change in SSID

Examples: `Device Id AP_00-0A-F5-00-01-B6 radio 4 disabled`

See Also: `<List of other alarms>`

Wireless: BSS Enabling Failed

Notification which indicates that the AP radio (BSS) enabling failed.

Syntax: “Bss enabling failed for DeviceId %s radio %d CauseCode %d”

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
Cause Code	Reason for AP radio enabling failure

Alarm Severity

Severity	Critical

Description: Notification which indicates that AP rado enabling has failed

Usage: The AP radio enabling can fail for reasons which are indicated by the Cause code parameter:

0 – Unspecified reason

1 – System timeout attempting to enable BSS.

Examples: `Bss enabling failed for Device Id AP_00-0A-F5-00-01-B6 radio 4 Cause Code 1`

See Also: `<List of other alarms>`

Wireless: Frequency Changed

Notification which indicates that the frequency of operation changed on the AP.

Syntax: "Frequency changed for DeviceId %s radio %d channelId %d CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP

Radio	Identifies Radio by interface ID on the Access Point
Channel ID	This indicates the channel on which the AP is operating.
Cause Code	Reason why frequency changed
Alarm Severity	
Severity	Critical

Description: This is a notification generated when operating frequency is changed for an AP radio due to either user triggers or events such as peridic DFS. The reason code can have an value of 0 which is unspecified reason. The new channel ID is also provided.

Reason Code	Description
0	Triggered due to DFS
1	User Triggered

Usage: This is an informational log.

Examples:

```
Frequency Changed for Device ID AP_00-0A-F5-00-01-B6 radio 4  channelId 64
CauseCode 0
```

See Also:

Wireless: STA Association Failed

Notification which indicates that the association failed for a 802.11 station.

Syntax: "Station association failed for DeviceId %s radio %d station MAC %s station status %d CauseCode"

Alarm Parameters	
DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
STA MAC Address	MAC address of 802.11 station.
STA status	Association or reassociation
Cause Code	Reason why station association failed
Alarm Severity	
Severity	Critical

Description: This is a notification generated when a association from a 802.11 station fails with the AP radio. The reasons for the failure are encapsulated in the cause code parameter and are as follows:

1 - Invalid parameters received from station in association request
2 - Only stations are allowed to associate with this AP based on current configuration
3 - Only backhauls can be formed with this AP based on current configuration
4 - Max backhaul limit is reached based on the 'Max Trunks' configuration for AP Admission Criteria
5 - Max station limit is reached based on the 'Max Stations' configuration for SSID
6 - SSID received in association request does not match SSID in AP configuration. This can occur more often when AP is not broadcasting SSID in beacon (either due to SSID being surpressed or multiple SSIDs being configured) and station is associating with AP with a different SSID.
7 - Authentication and encryption requested by station does not match security policy of the AP
8 - Multi Vendor Station are not allowed to associate based on AP Admission Criteria
9 - 802.11b stations are not allowed to associate based on AP Admission Criteria
10 - Station is not allowed to associate and transferred to another AP Radio due to Load Balancing
11 - Station is not allowed to associate because node does not have network connectivity

Usage: The reason for the association failure can be used to determine any configuration issue in the system which may be causing the association failures.

Examples:

```
Station association failed for Device ID AP_00-0A-F5-00-01-B6 radio 4  station MAC
00:0a:f5:00:3a:fe CauseCode 2
```

See Also:

Wireless: STA Associated

Notification which indicates that the association and authentication was successful for a 802.11 station.

Syntax: "Station associated for DeviceId %s radio %d station MAC %s, Station status %d userId %s station count %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
STA MAC Address	MAC address of 802.11 station.
STA status	Association or reassociation
User ID	Identifies user by user name or MAC address
Station Count	Current count of associated users with AP.

Alarm Severity

Severity	Critical

Description: This is a notification generated when a association and authentication from a 802.11 station succeeds with the AP radio. In addition count of current associated stations, type of association and user ID is provided. User ID is user name if RADIUS authentication is used and MAC address otherwise.

Usage: Informational log.

Examples:

```
Station associated for Device ID AP_00-0A-F5-00-01-B6 radio 4  station MAC
00:0a:f5:00:3a:fe, Station status 1 userId John Doe station count 10
```

See Also:

Wireless: STA Disassociated

Notification which indicates that a 802.11 station disassociated.

Syntax: "Station disassociated from AP for DeviceId %s radio %d station MAC %s CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
STA MAC Address	MAC address of 802.11 station.
Cause Code	Reason Code for disassociation

Alarm Severity

Severity	Critical

Description: This is a notification generated when a 802.11 station is disassociated either by the network or the station.

Reason Code	Description
0	STA initiated disassociation
1	Station has handed off to another AP
2	Disassociation triggered due to authentication failure after ULAP timeout
3	Disassociation triggered due to user action.

Usage: Informational log.

Examples:

```
Station disassociated for Device ID AP_00-0A-F5-00-01-B6 radio 4  station MAC
00:0a:f5:00:3a:fe, CauseCode 0
```

See Also:

Wireless: WDS Failed

Notification which indicates a failure in formation of Wireless Backhaul

Syntax: "WDS trunk brought down for DeviceId %s radio %d remote MAC %s CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
Remote MAC Address	MAC address of remote end of backhaul link
Cause Code	Reason Code for WDS formation failure

Alarm Severity

Severity	Critical

Description: This is a notification generated when a wireless backhaul formation fails. The remote end’s MAC address is provided. This notification is generated by AP node.

Reason Code	Description
0	System Failure
1	Maximum BP count has been reached (this relevant only for AP)
2	Join attempt to the uplink AP failed (relevant only on BP side)

Usage: This can be used to track any losses in connectivity of network.

Examples:

```
WDS trunk brought down for Device ID AP_00-0A-F5-00-01-B6 radio 4  remote MAC
00:0a:f5:00:3a:fb, CauseCode 0
```

See Also:

Wireless: WDS Up

Notification which indicates successful formation of wireless backhaul

Syntax: "WDS trunk established for DeviceId %s radio %d remote mac %s TrunkPort count %d CauseCode %d”

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP

Radio	Identifies Radio by interface ID on the Access Point
Remote MAC Address	MAC address of remote end of backhaul link
Backhaul Count	Number of backhauls which are formed to this AP radio
Cause Code	Indicates whether backhaul was a retrunk or not

Alarm Severity

Severity	Critical

Description: This is a notification generated when a wireless backhaul formation succeeds. The remote end's MAC address is provided.

Reason Code	Description
0	Trunk has been established
1	Trunk has been optimized (re-established based on better connectivity)

Usage: Informational log

Examples:

```
            WDS trunk established for Device ID AP_00-0A-F5-00-01-B6 radio 4
remote MAC 00:0a:f5:00:3a:fb TrunkPort count 2 CauseCode 0
```

See Also:

Wireless: WDS Down

Notification which indicates that a wireless backhaul link has gone down

Syntax: "WDS trunk brought down for DeviceId %s radio %d remote MAC %s CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
Remote MAC Address	MAC address of remote end of backhaul link
Cause Code	Indicates why backhaul link was bought down

Alarm Severity

Severity	Critical

Description: This is a notification generated when a wireless backhaul has gone down. The remote end's MAC address is provided.

Reason Code	Description
0	System Reason (unspecified)

1	Loss of Link (applies to BP side only)
2	Trunk brought down by uplink AP (applies to BP side only)
3	User retrunk issued (this can occur due to new backhaul configuration being applied on BP)
4	Trunk has reformed with another AP (AP side only)
5	Trunk brought down by BP (applies to AP side only)

Usage: Informational log

Examples:
```
WDS trunk brought down for Device ID AP_00-0A-F5-00-01-B6 radio 4  remote MAC
00:0a:f5:00:3a:fb CauseCode 0
```

See Also:

Security: Guest Authentication Succeeded

Notification which indicates that a “Guest Access” Station has been successfully authenticated

Syntax: "For device-id %s , Guest authentication succeeded for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the “Landing Page” that has accomplished authentication of the Guest STA. This is either simply the Internal “Landing Page”, or a URL identifying the “External Landing Page” which performed the authentication.
Guest Mode	Currently, always set to 4.

Alarm Severity

Severity	Normal

Description: Notification which is generated when a “Guest Station” is authenticated.

Usage: This indicates the successful start of a “Guest Access” Stations communications session. This Guest STA will be offered the communications services specified in the Guest Profilethat has been configured for the specified SSID.

Examples:
```
For device-id AP_00-0A-F5-00-01-89 , Guest authentication succeeded for STA
00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and
guest mode 4
```

See Also: `Security: Guest Authentication Failed`

Security: Guest Authentication Failed

Notification which indicates that a “Guest Access” Station has failed authentication

Syntax: "For device id %s, Guest authentication failed for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d due to %d"

Alarm Parameters	
DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the “Landing Page” that has accomplished authentication of the Guest STA. This is either simply the Internal “Landing Page”, or a URL identifying the “External Landing Page” which performed the authentication.
Guest Mode	Currently, always set to 4.
Reason code	Currently, always set to 0.
Alarm Severity	
Severity	Critical

Description: Notification which is generated when a “Guest Station” fails authentication.

Usage: This indicates that a Guest Station did not present the appropriate “credentials” (currently simple password) upon request.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , Guest authentication failed for STA
00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and
guest mode 4 due to 0
```

See Also: `Security: Guest Authentication Succeeded`

Security: User rejected by RADIUS Server

Notification which indicates that the AP has determined that a User has been rejected by RADIUS.

Syntax: "For device-id %s, the RADIUS SERVER %s:%d from auth zone %s rejected the STA %s on radio %d with user-id %s and SSID %s"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Auth Zone	The name of the Auth Zone on this AP that this RADIUS server is a member of
Station	MAC address of the Station
Radio	Identifies Radio by interface ID on the Access Point
User ID	The Username
SSID	Identifies the SSID on this AP that the STA has associated with

Alarm Severity

Severity	Critical

Description: This notification is generated when a User authentication fails. The context of the AP radio and the RADIUS server which rejected the User are also provided.

Usage: This indicates that the AP has determined that RADIUS has rejected a user authentication attempt.

Examples: For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 from auth zone BldgOne rejected rejected the STA 00:0a:f5:00:05:cc on radio 0 with user-id paul and SSID NewYorkRm

See Also:

Security: BP rejected by RADIUS Server

Notification which indicates that the AP has determined that a RADIUS server has rejected this BP’s authentication attempt.

Syntax: "For device-id %s, the RADIUS SERVER %s:%d from auth zone %s rejected the node %s on radio %d with device-id %s and SSID %s"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Auth Zone	The name of the auth Zone on this AP that this RADIUS server is a member of

Node	MAC address of the BP node
Radio	Identifies Radio by interface ID on the Access Point
Device ID	The Device ID of the BP node
SSID	Identifies the SSID on this AP that the STA has associated with

Alarm Severity

Severity	Critical

Description: This notification is generated when a Bridge Portal (radio) authentication fails. The context of the BP radio and the RADIUS server which rejected the BP radio are also provided. A BP attempts authentication when a wireless backhaul is being established.

Usage: This indicates that a security portal has rejected a BP's authentication attempt with this AP. Usually it means that the BP is not enrolled in the same network as the AP. It may also mean that the BP was just enrolled, and the enrollment database has not yet been synced across the network to all security portals.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 from
auth zone BldgOne rejected the node 00:0a:f5:00:06:22 on radio 0 with device-id AP_00-
0A-F5-00-01-89 and SSID NewYorkRm
```

See Also:

Security: RADIUS Server timeout

Notification which indicates that the AP has determined that a RADIUS server has failed to respond within the RADIUS timeout.

Syntax: "For device-id %s, the RADIUS server %s:%d from auth zone %s failed to respond within %d seconds and %d attempts while authenticating STA %s on radio %d with user-id %s and SSID %s"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Auth Zone	The name of the auth Zone on this AP that this RADIUS server is a member of
RADIUS timeout	The current setting of the RADIUS timeout.
RADIUS retries	The number of retries performed
Station	MAC address of the Station.

Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID established during EAPOL Authentication exchange
SSID	Identifies the SSID on this AP that the STA has associated with

Alarm Severity

Severity	Critical

Description: This notification is generated when the RADIUS server fails to respond within a certain timeout period.

Usage: This indicates that the AP has determined that a RADIUS server has failed to respond within the RADIUS timeout. This may mean that the RADIUS server is unreachable over the network, or the shared secret with the RADIUS server is misconfigured on the AP. Usually, RADIUS servers do not respond when clients attempt to communiate with bad shared secrets. If multiple RADIUS servers are configured in this auth zone, the AP will switch to using the next one in the list.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 from
auth zone BldgOne failed to respond within 5 seconds and 3 attempts while authenticating
STA 00:0a:f5:00:05:f0 on radio 0 with user-id paul and SSID NewYorkRm
```

See Also:

Security: Management User login success

Notification which indicates that the AP has determined that a Management user login has succeeded.

Syntax: "For device-id %s, the management user '%s' with privilege level %d logged in succesfully via %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Management User	Username of management User.
Privilege Level	The privilege level of the management user (Ignore in this release.)
Login access	Identifies the type of access, console, or SSH. (Ignore in this release.)

Alarm Severity

Severity	Critical

Description: This notification is generated whenever a management User tries to login to the local AP.

Usage: This indicates that the AP has determined that a Management user login has succeeded.

Examples: For device-id AP_00-0A-F5-00-01-89 , the management user 'admin' with privilege level 1 logged in succesfully via 1

See Also:

Security: Management User login failure

Notification which indicates that the AP has determined that a Management user login has failed.

Syntax: "For device-id %s, the management user '%s' failed to login successfully via %d”

DeviceId	The Device ID of the 108 Mbps Wireless AP
Management User	Username of management User.
Login access	Identifies the type of access, console, or SSH. (Ignore in this release.)
Alarm Severity	
Severity	Critical

Description: This notification is generated when a management User login attempt is unsuccessful.

Usage: This indicates that the AP has determined that a Management user login has failed. Too many failed logins in succession might attempt that someone is trying to break into your AP.

Examples: For device-id AP_00-0A-F5-00-01-89 , the management user 'admin' failed to login successfully via 1

See Also:

Security: STA failed EAPOL MIC check

Notification which indicates that the AP has determined that a STA has failed a MIC check during the EAPOL authentication exchange.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user-id %s and SSID %s failed an EAPOL-MIC check with auth-type %d during key exchange %d. (If using WPA-PSK, check the PSK on the STA.)"

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point

User	Supplicant User ID established during EAPOL Authentication exchange
SSID	Identifies the SSID on this AP that the STA has associated with
Authentication Type	The valid types include: WPA PSK (3), WPA EAP (4)
Key Exchange	0 for pairwise key exchange, and 1 for group key exchange.

Alarm Severity

Severity	Critical

Description: This notification is generated when the MIC fails during EAPOL key exchange process.

Usage: This indicates that the AP has determined that a STA has failed a MIC check during the EAPOL authentication exchange. If the authentication type is WPA PSK, and the failure happened during the pairwise key exchange, then this is most likely due to a misconfiguration of the WPA pre-shared key on the station. Otherwise, it might mean that an attacker's station is attempting to marquerade as a legal station.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm failed an EAPOL-MIC check with auth-type 4 during key exchange 2. (If using WPA-PSK, check the PSK on the STA.)

See Also:

Security: STA attempting WPA PSK – no Pre-shared Key is set for SSID

Notification which indicates that the AP has determined that a STA is attemping WPA-PSK authentication – but no Pre-shared Key has been configured for the SSID.

Syntax: "For device-id %s, the STA %s on radio %d attempted to do WPA-PSK based auth on the SSID %s but no pre-shared key is set."

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the STA has associated with

Alarm Severity

Severity	Critical

Description: This notification is sent when a Station attempts to do a WPA-PSK based authentication on a given SSID, but no WPA pre-shared key is setup for that SSID.

Usage: This indicates that the AP has determined that a STA is attempting to perform WPA-PSK authentication – but no WPA Pre-shared Key has been configured on this AP for that SSID. Recall that WPA PSK's are configured per SSID.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 on radio 0 attempted to
do WPA-PSK based auth on the SSID NewYorkRm but no pre-shared key is set.
```

See Also:

Security: Auth Server Improperly configured on this SSID

Notification which indicates that the AP has determined that a STA requires authentication servers – and these are not configured properly on this SSID.

Syntax: "For device-id %s, Auth servers are improperly configured for the SSID %s and are needed for authenticating STA %s on radio %d with RADIUS usage %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
SSID	Identifies the SSID on this AP that the STA has associated with
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
RADIUS Usage	A code indicating what the RADIUS server was required for: Legacy 8021.x for dynamic WEP (1), WPA EAP athentication (2), MAC address based ACL lookup (3).

Alarm Severity

Severity	Critical

Description: This notification is sent when authentication servers are improperly configured for a given SSID.

Usage: This indicates that the AP has determined that a STA requires authentication servers configured –and there are none configured on this SSID Generally authentication servers are needed for EAP based authentication, or for MAC address based ACL lookups.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , Auth servers are improperly configured for the
SSID NewYorkRm and are needed for authenticating STA 00:0a:f5:00:05:f0 on radio 0
with RADIUS 2
```

See Also:

Security: STA failed to send EAPOL-Start

Notification which indicates that the STA has failed to send an EAPOL-Start even though it was expected to for EAP based authentication.

Syntax: "For device-id %s, the STA %s on radio %d and SSID %s failed to send an EAPOL-Start in order to begin auth of type %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the STA has associated with
Authentication Type	The valid types include: LEGACY 8021.x (2), WPA EAP (4)

Alarm Severity

Severity	Critical

Description: This notification is sent during authentication, when the Station fails to send an EAPOL-Start in order to begin the authentication using WPA-EAP or legacy 802.1X protocols.

Usage: This indicates that the AP has determined that a STA has failed to send an EAPOL-Start. This might indicate a misconfiguration on the STA. The AP expects the STA to send an EAPOL-Start if the authentication type is deemed to be EAP based. This can happen when WPA EAP authentication is negotiated, or when WEP is enabled on the AP and no manual WEP keys are configured.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 on radio 0 and SSID
NewYorkRm failed to send an EAPOL-Start in order to begin auth of type 4
```

See Also:

Security: RADIUS sent a bad response

Notification which indicates that the AP has determined that a RADIUS server has sent a bad response.

Syntax: "For device-id %s, the RADIUS server %s:%d sent back a bad response due to %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP

RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Response	The reason codes for the bad response: BAD SIGNATURE BASED ON SHARED SECRET (0), UNEXPECTED RESPONSE TYPE WHEN DOING EAP AUTH (1), UNEXPECTED RESPONSE TYPE WHEN DOING MAC-ACL LOOKUP (2), LEGAL MS-MPPE KEYS NOT PRESENT (3), BAD ENCODING FOR USER GROUP ATTRIBUTE (5)

Alarm Severity

Severity	Critical

Description: This notification is sent during authentication, when the RADIUS server sends a bad response. The aniNotifCauseCode identifies the reason associated with this bad response.

Usage: This indicates that the AP has determined that a RADIUS server has sent a bad or unexpected response. The response could be bad because the cryptographic signature check might have failed or because an attribute might be missing or badly encoded.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 sent
back a bad response due to 7
```

See Also:

Security: RADIUS timeout too short

Notification which indicates that the AP has determined that a RADIUS server has sent a late response. This indicates that the APs RADIUS timeout might need to be increased.

Syntax: "For device-id %s, the RADIUS server %s:%d sent a late response - you might need to increase your RADIUS timeout of %d seconds"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
RADIUS timeout	The current setting of the RADIUS timeout.

Alarm Severity

Severity	Critical

Description: This notification is generated when the AP receives a late response from the

RADIUS server, as opposed to not receiving any response at all. The AP may have attempted multiple retries or may even have switched to another RADIUS server by this time. This indicates that due to higher latencies in the network, it might be better to increase the timeout associated with the authentication server.

Usage: This indicates that the AP has determined that a RADIUS server has sent a late response.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 sent a
late response - you might need to increase your RADIUS timeout of 4 seconds
```

See Also:

Security: STA authentication did not complete in time

Notification which indicates that the AP has determined that a station has failed to complete the proper sequence of authentication exchanges in a timely manner.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not complete its auth sequence in time with auth-type %d and enc-type %d due to reason code %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
AP	The MAC address of the upstream AP.
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID, if exchanged the during EAPOL authentication
SSID	Identifies the SSID on this AP that the STA has associated with
Authentication Type	The valid types include: LEGACY 802.1x (2), WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)
Reason Code	The reason for the failure: EAP-REQUEST NOT RECEIVED FROM AUTHENTICATION SERVER (2)

Alarm Severity

Severity	Critical

Description: This notification is generated when the station authentication sequence did not complete in time.

Usage: This indicates that the AP has determined that the station authentication sequence did not complete in time.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not complete its auth sequence in time with auth-type 4 and enc-type 6 due to reason code 6

See Also: `EAP User-ID timeout, EAP Response Timeout`

Security: Upstream AP is using an untrusted auth server

Notification which indicates that the local BP has determined that the upstream AP is using an untrusted auth server.

Syntax: "For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d is using an untrusted auth server %s with certificate SHA-1 thumbprint %s : IT MIGHT BE A ROGUE AP”

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point
Node	The Device ID (X.509 Certificate CN) of the entity used by the upstream AP as an auth server
Thumbprint	The SHA-1 Thumbprint of the certificate for this purported portal

Alarm Severity

Severity	Critical

Description: This notification is generated when the local BP has determined that the upstream AP is using an un-trusted auth server.

Usage: This indicates that the local BP has determined that the upstream AP is using an un-trusted auth server. This may indicate that the upstream AP is a rogue AP. It is safe to say that the upstream AP and the downstream AP are not enrolled in the same network. If the downstream AP was previously enrolled elsewhere, then reset it and re-enroll it in the new network.

Examples: For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 is using an untrusted auth server 00:0a:f5:00:01:45 with certificate SHA-1 thumbprint 98:72:a8:6d:56:f8:92:a8:f3:97:ec:3f:fa:0b:66:4e : IT MIGHT BE A ROGUE AP

See Also:

Security: Upstream AP is using a non-portal node as its auth server

Notification which indicates that the local BP has determined that the upstream AP is using a non-portal node as an auth server.

Syntax: "For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d is using a non portal node %s with certificate SHA-1 thumbprint %s as its auth server: YOUR ENROLLMENT DATABASE MIGHT BE OUT OF SYNC."

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point
Node	The Device ID (X.509 Certificate CN) of the entity used by the upstream AP as an auth server
Thumbprint	The SHA-1 Thumbprint of the certificate for this purported portal

Alarm Severity

Severity	Critical

Description: This notification is generated when the local BP has determined that the upstream AP is using a node that is not a security portal as its auth server. This indicates that the BP knows about the other PLANEX node, but does not believe it is authorized to be a Security Portal.

Usage: This indicates that the local BP has determined that the upstream AP is out-of-sync with respect to the identity of legitimate portal APs and the enrollment databases are out of sync on the downstream AP and the upstream AP.

Examples: For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 is using a non portal node 00:0a:f5:00:01:45 with certificate SHA-1 thumbprint 98:72:a8:6d:56:f8:92:a8:f3:97:ec:3f:fa:0b:66:4e as its auth server: YOUR ENROLLMENT DATABASE MIGHT BE OUT OF SYNC

See Also:

Security: Upstream AP failed MIC check during BP authentication

Notification which indicates that the local BP has determined that the upstream AP has failed a MIC check on a received frame.

Syntax: "For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d failed an EAPOL-MIC check with auth-type %d during key exchange %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point
Authentication Type	The valid types include: RSN PSK (3), RSN EAP (4)
Key Exchange	Pairwise key exchange (0), group ky exchange (1).

Alarm Severity

Severity	Critical

Description: This notification is generated when the MIC fails during EAPOL key exchange process via a BP radio.

Usage: This indicates that a frame with a MIC failure has been received during the EAPOL Key Exchange process.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID
NewYorkRm authenticating via local BP radio 0 failed an EAPOL-MIC check with auth-type
4 during key exchange 3
```

Security: Premature EAP-Success received

Notification which indicates that the local BP has recevied an EAP-Success BEFORE authentication has completed.

Syntax: "For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d sent EAP-Sucess before authentication completed : IT MIGHT BE A ROGUE AP"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical

Description: This notification is generated when an upstream AP sends an EAP success before authentication is completed. This may be a rogue AP trying to force an AP to join even before authentication is complete.

Usage: This indicates that the local BP has received an EAP-Success before authentication has even been completed.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID
NewYorkRm authenticating via local BP radio 0 sent EAP-Sucess before authentication
completed : IT MIGHT BE A ROGUE AP
```

See Also:

Security: Profile not configured for user-group

Notification which indicates that the AP has determined that a STA is a member of group for which a corresponding service profile has NOT been configured in this SSID.

Syntax: "For device-id %s, the STA %s on radio %d with user %s is in group %s but SSID %s has no profile configured for that group"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
User	User ID
Group	Group tag for this user (determined from RADIUS configuration)
SSID	Identifies the SSID on this AP that the STA has associated with.

Alarm Severity

Severity	Critical

Description: This notification is generated during Station authentication when no service profile has been configured for a given Group.

Usage: This indicates that the AP has detected a STA is authenticating which is a member of a group for which no service profile has yet been configured in this SSID.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:cc  on radio 0 with user
paul is in group employee but SSID NewYorkRm has no profile configured for that group.
```

See Also:

Security: STA has failed security enforcement check

Notification which indicates that the AP has determined that a STA has failed the security enforcement checks for its service profile.

Syntax: "For device-id %s, the STA %s on radio %d with user %s and SSID %s of group %s failed the security enforcement check with auth-type %d and enc-type %d at enforcement level %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID
SSID	Identifies the SSID on this AP that the STA has associated with.
Group	Group tag for this user (determined from RADIUS configuration)
Authentication Type	The valid types include: NONE (0), SHARED KEY (1), LEGACY EAP (2), RSN PSK (3), RSN EAP (4)
Encryption Type	The valid types include: NONE (0), WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)
Enforcement Level	The security enforcement level configured in the service profile: AES ONLY (1) TKIP OR AES (2), WEP ONLY (3), NO ENCRYPTION (4), DEFAULT ENFORCEMENT (5)

Alarm Severity

Severity	Critical

Description: This notification is generated if the STA fails the security enforcement checks for its service profile

Usage: This indicates that the STA is attempting to use an encryption type that is not allowed in its service profile. The service profile is determined based on the SSID and user group of the STA. Note that the AP may advertize multiple encryption capabilities, but different STAs might be restricted to different subsets of encryption capabilities based on their service profiles.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:cc  on radio 0 with user paul and SSID NewYorkRm of group employee failed the security enforcement check with auth-type 4 and enc-type 5 at enforcement level 1
```

See Also:

Security: Guest Authentication Succeeded

Notification which indicates that a "Guest Access" Station has been successfully authenticated

Syntax: "For device-id %s , Guest authentication succeeded for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the "Landing Page" that has accomplished authentication of the Guest STA. This is either simply the Internal "Landing Page", or a URL identifying the "External Landing Page" which performed the authentication.
Guest Mode	Currently, always set to 4.

Alarm Severity

Severity	Critical

Description: Notification which is generated when a "Guest Station" is authenticated.

Usage: This indicates the successful start of a "Guest Access" Stations communications session. This Guest STA will be offered the communications services specified in the Guest Profilethat has been configured for the specified SSID.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , Guest authentication succeeded for STA
00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and
guest mode 4
```

See Also: `Security: Guest Authentication Failed`

Security: Guest Authentication Failed

Notification which indicates that a "Guest Access" Station has failed authentication

Syntax: "For device id %s, Guest authentication failed for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d due to %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP

Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the "Landing Page" that has accomplished authentication of the Guest STA. This is either simply the Internal "Landing Page", or a URL identifying the "External Landing Page" which performed the authentication.
Guest Mode	Currently, always set to 4.
Reason code	Currently, always set to 0.

Alarm Severity

Severity	Critical

Description: Notification which is generated when a "Guest Station" fails authentication.

Usage: This indicates that a Guest Station did not present the appropriate "credentials" (currently simple password) upon request.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , Guest authentication failed for STA
00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and
guest mode 4 due to 0
```

See Also: `Security: Guest Authentication Succeeded`

Security: AP Detected Bad TKIP MIC

Notification which indicates that the AP has detected a BAD TKIP MIC value in an incoming frame encrypted with the pairwise/uniast key.

Syntax: "For device-id %s, a bad TKIP MIC was detected on an incoming unicast packet from STA %s on radio %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical

Description: This notification is generated when a bad TKIP MIC is detected on an incoming frame from a STA that is ecrypted with the pairwise/unicast key.

Usage: This indicates that the AP has detected an invalid TKIP MIC value on an incoming frame. All packets received by the AP are always encrypted with the pairwise/unicast key.

Examples: For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected on an incoming unicast packet from STA 00:0a:f5:00:05:cc on radio 0

See Also:

Security: BP Detected Bad TKIP MIC on Incoming Unicast

Notification which indicates that the BP has detected a BAD TKIP MIC value in an incoming frame from the AP that is encrypted with the pairwise/unicast key.

Syntax: "For device-id %s, a bad TKIP MIC was detected by local BP radio %d on an incoming unicast packet from the AP %s"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
AP MAC address	The MAC address of the source AP

Alarm Severity

Severity	Critical

Description: This notification is generated when a bad TKIP MIC is detected by a local BP radio, identified by aniApRadioIndex, on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.

Usage: This indicates that the BP has detected an invalid TKIP MIC value on an incoming frame encrypted with the pairwise/unicast key.

Examples: For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by local BP radio 0 on an incoming unicast packet from the AP 00:0a:f5:00:06:22

See Also: BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast

Security: BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast

Notification which indicates that the BP has detected a BAD TKIP MIC value in an incomng frame from the AP that is encrypted with the group/multicast/broadcast key.

Syntax: "For device-id %s, a bad TKIP MIC was detected by local BP radio %d on an incoming multicast/broadcast packet from the AP %s"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Radio	Identifies Radio by interface ID on the Access Point
AP MAC address	The MAC address of the source AP

Alarm Severity

Severity	Critical

Description: This notification is generated when a bad TKIP MIC is detected by a local BP radio, identified by aniApRadioIndex, on an incoming multicast or broadcast packet from the AP where the packet is encrypted with the group/multicast/ broadcast key..

Usage: This indicates that the BP has detected an invalid TKIP MIC value on a received multicast/broadcast frame.

Examples: For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by local BP radio 0 on an incoming multicast/broadcast packet from the AP 00:0a:f5:00:06:22

See Also: `BP Detected Bad TKIP MIC on Incoming Unicast`

Security: STA Detected Bad TKIP MIC on Incoming Unicast

Notification which indicates that a STA associated with this AP has detected a BAD TKIP MIC value in a frame it received from the AP encrypted with the pairwise/unicast key.

Syntax: "For device-id %s, a bad TKIP MIC was detected by STA %s on radio %d on an incoming unicast packet from the AP"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical

Description: This notification is generated when a bad TKIP MIC is detected by an STA associated with this AP on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.

Usage: This indicates that the STA has detected an invalid TKIP MIC value on an incoming frame encrypted with the pairwise/unicast key.

Examples: For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by STA 00:0a:f5:00:05:f0 on radio 0 on an incoming unicast packet from the AP

See Also: `STA Deteted Bad TKIP MIC on Incoming Multicast/Broadcast`

Security: STA Detected Bad TKIP MIC on Incoming Multicast/Broadcast

Notification which indicates that a STA associated with this AP has detected a BAD TKIP MIC value in a multicast/broadcast frame it received from the AP.

Syntax: "For device-id %s, a bad TKIP MIC was detected by STA %s on radio %d on an incoming multicast/broadcast packet from the AP"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical

Description: This notification is generated when a bad TKIP MIC is detected by an STA associated with a radio, identified by aniApRadioIndex, on an incoming multicast or broadcast packet from the AP where the packet is encrypted with the group/ multicast/broadcast key.

Usage: This indicates that the STA has detected an invalid TKIP MIC value on a received, multicast, frame.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by STA
00:0a:f5:00:05:f0 on radio 0 on an incoming multicast/broadcast packet from the AP
```

See Also: `STA Detected Bad TKIP MIC on Incoming Unicast`

Security: TKIP counter-measures lockout period started

Notification which indicates that the AP is taking active counter-measures against an attempted compromise of TKIP.

Syntax: "For device-id %s, the TKIP counter-measures lockout period has started for 60 seconds."

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP

Alarm Severity

Severity	Critical

Description: This notification is generated when a TKIP counter measures lockout period for 60 seconds is started.

Usage: This indicates that the AP has determined that an attempt is underway to compromise the secure operation of TKIP. This happens if two MIC failures are detected within a 60 second interval. If this happens, the AP disassociates all STAs and prevents new STAs from associating for a period of 60 seconds.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the TKIP counter-measures lockout period has
started for 60 seconds.
```

See Also:

Security: EAP User-ID timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with its User-ID during the authentication exchange.

Syntax: "For device-id %s, the STA %s[%d] on radio %d and SSID %s did not send its user-id in time to complete its auth sequence with auth-type %d and enc-type %d."

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: LEGACY 8021.x (2), WPA EAP (4)
Encryption Type	The valid types include: WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)

Alarm Severity

Severity	Critical

Description: This notification is generated when an STA fails to send its user-id in time to complete its authentication sequence using the specified authentication type.

Usage: This indicates the failure of a STA to complete the EAP authentication exchange in a timely fashion. The two authentication modes that require the STA to send its user-id are WPA EAP and legacy 8021.x for dynamic WEP. This trap might indicate that a user prompt is not attended to on the client side.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 and SSID
NewYorkRm did not send its user-id in time to complete its auth sequence with auth-type
4 and enc-type 6
```

See Also: `EAP Response Timeout, STA Authentication Timeout`

Security: EAP response timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with an EAP response during the authentication exchange.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send an EAP-Response in time to complete its auth sequence with auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID established during EAPOL Authentication exchange
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: LEGACY 802.1x (2), WPA EAP (4)
Encryption Type	The valid types include: WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)

Alarm Severity

Severity	Critical

Description: This notification is generated when an STA fails to send an EAP-Response in time to complete its authentication sequence using the specified authentication type and encryption. This is an EAP response other that the User-ID.

Usage: This indicates the failure of a STA to complete its EAP authentication exchange in a timely fashion.The two authentication modes that require the STA to send EAP responses are WPA EAP and legacy 8021.x for dynamic WEP. This trap might indicate that a user prompt is not attended to on the client side. It may also indicate that the client silently rejected a EAP request sent from the RADIUS server – perhaps because it did not trust the RADIUS server’s credentials.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send an EAP-Response in time to complete its auth sequence with auth-type 4 and enc-type 6

See Also: `EAP User-ID Timeout, STA Authentication Timeout`

Security: EAPOL Key exchange – message 2 timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with EAPOL 4-way handshake message number 2.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Pairwise Messg #2 in time where auth-type %d and enc-type %d"

Alarm Parameters	
DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	User ID established during EAPOL Authentication exchange (if applicabe)
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: TKIP (5), AES (6)
Alarm Severity	
Severity	Critical

Description: This notification is generated when an STA fails to send the WPA EAPOL-Key Pairwise Message #2 in time to complete the pairwise key exchange.

Usage: This indicates the failure of a STA to complete the EAPOL 4-way key exchange in a timely fashion.

Examples:

```
For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user
paul and SSID NewYorkRm did not send the WPA EAPOL-Key Pairwise Messg #2 in time
where auth-type 4 and enc-type 6
```

See Also:

Security: EAPOL Key exchange – message 4 timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with EAPOL 4-way handshake message number 4.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Pairwise Messg #4 in time where auth-type %d and enc-type %d"

Alarm Parameters	
DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	User ID established during EAPOL Authentication exchange (if applicable)
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include:WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: TKIP (5), AES (6)
Alarm Severity	
Severity	Critical

Description: This notification is generated when an STA fails to send the WPA EAPOL-Key Pairwise Message #4 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.

Usage: This indicates the failure of a STA to complete the EAPOL 4-way key exchange in a timely fashion.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Pairwise Messg #4 in time where auth-type 4 and enc-type 6

See Also:

Security: EAPOL Group 2 key exchange timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with EAPOL Group key exchange message number 2.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Group Messg #2 in time where auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The Device ID of the 108 Mbps Wireless AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	User ID established during EAPOL Authentication exchange (if applicable)
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: TKIP (5), AES (6)

Alarm Severity

Severity	Critical

Description: This notification is generated when an STA fails to send the WPA EAPOL-Key Group Message #2 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.

Usage: This indicates the failure of a STA to complete the Group Key exchange in a timely fashion.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Group Messg #2 in time where auth-type 4 and enc-type 6

See Also:

Glossary

This glossary defines terms that apply to wireless and networking technology in general and PLANEX products in particular.

802.1x

Standard for port-based authentication in LANs. Identifies each users and allows connectivity based on policies in a centrally managed server.

802.11

Refers to the set of WLAN standards developed by IEEE. The three commonly in use today are 802.11a, 802.11b, and 802.11g, sometimes referred to collectively as Dot11.

Access Control List (ACL)

A list of services used for security of programs and operating systems. Lists users and groups together with the access awarded for each.

Access Point (AP)

An inter-networking device that connects wired and wireless networks together. Also, an 802.11x capable device that may support one or more 802.11 network interfaces in it and co-ordinates clients stations in establishing an Extended Service Set 802.11 network

Advanced Encryption Standard (AES)

An encryption algorithm developed for use by U.S. Government agencies and now incorporated into encryption standards for commercial transactions.

Ad-Hoc network

A group of nodes or systems communicating with each other without an intervening Access Point. Many wireless network cards support ad-hoc networking modes.

Authentication Server

A central resources that verifies the identity of prospective network users and grants access based on pre-defined policies.

Authentication Zone

A administrative grouping of resources for user authentication.

Backhaul

The process of getting data from a source and sending it for distribution over the main backbone network. Wireless backhaul refers to the process of delivering data from a node on the wireless network back to the wired network. Also referred to a WDS.x.

Basic Service Set (BSS)

The set of all wireless client stations controlled by a single access point. The BSSID, or identifier, for the basis service set can be assigned or default to the MAC address of the access point.

Bridge

A connection between two (or more) LANs using the same protocol. Virtual bridges are used as a means of defining layer 2 domains for broadcast messages. Each virtual bridge uniquely defines a virtual local area network (VLAN).

Class of Service (COS)

A method of specifying and grouping applications into various QoS groups or categories.

Differentiated Services Code Point (DSCP)

A system of assigning Quality of Service "Class of Service" tags.

Domain Name Service (DNS)

A standard methodology for converting alphanumeric Internet domain names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)

A communications protocol enabling IP address assignments to be managed both dynamically and centrally. With DHCP enabled on a node (a system, device, network card, or Access Point), when it boots or is connected to a network, an address is automatically assigned. Each assigned address is considered to be "leased" to a specific node; when the lease expires, a new IP can be requested and/or automatically reassigned. Without DHCP, IP addresses would need to be entered manually for each and every device on the network.

Dynamic Frequency Selection (DFS)

A method for selecting the least intrusive and noisy available frequency for operation, part of the 802.11 specification.

Dynamic IP Address

A TCP/IP network address assigned temporarily (or dynamically) by a central server, also known as a DHCP server. A node set to accept dynamic IPs is said to be a "DHCP client."

Extensible Authentication Protocol (EAP)

Standard that specifies the method of communication between an authentication server and the client, or supplicant, requesting access to the network. EAP supports a variety of authentication methods.

Extensible Authentication Protocol Over LAN (EAPOL)

Protocol used for 802.1x authentication.

EAP-TLS

EAP using Transport Layer Security. EAP-based authentication method based on X.509 certificates, which provides mutual, secure authentication. Certificates must be maintained in the authentication server and supplicant.

EAP-PEAP

Protected EAP-based authentication method based on X.509 certificates. Uses a two-phase approach in which the server is first authenticated to the supplicant. This establishes a secure channel over which the supplicant can be authenticated to the server.

Extended Service Set (ESS)

A set of multiple connected BSSs. From the perspective of network clients, the

ESS functions as one wireless network, with clients able to roam between the BSSs within the ESS.

ESSID

Name or identifier of the ESS used in network configuration.

hostname

The unique, fully qualified name assigned to a network computer, providing an alternative to the IP address as a way to identify the computer for networking purposes.

Hypertext Transfer Protocol (HTTP)

Protocol governing the transfer of data on the World Wide Web between servers and browser (and browser enabled software applications).

Hypertext Transfer Protocol over SSL (HTTPS)

A variant of HTTP that uses SSL (Secure Sockets Layer) encryption to secure data transmissions. HTTPS uses port 443, as opposed to HTTP which uses port 80.

Independent Basic Service Set (IBSS)

A set of clients communicating with each other or a network via an Access Point.

Internet Protocol (IP)

The network layer protocol for routing packets through the Internet.

IP address

32-bit number, usually presented as a period-separated (dotted decimal) list of three-digit numbers, which identifies an entity on the Internet according to the Internet Protocol standard.

Local Area Network (LAN)

A group of computers, servers, printers, and other devices connected to one another, with the ability to share data between them.

Maskbits

Number of bits in the subnet prefix for an IP address, (provides the same information as subnet mask). Each triplet of digits in an IP address consists of 8 bits. To specify the subnet in maskbits, count the number of bits in the prefix. To specify using a subnet mask, indicate the masked bits as an IP address. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Media Access Control (MAC) Address

A unique hardware-based equipment identifier, set during device manufacture. The MAC address uniquely identifies each node of a network. Access Points can be configured with MAC access lists, allowing only certain specific devices to connect with the LAN through them, or to allow certain MAC-identified network cards or devices access only to certain resources.

MAC address authentication

Method of authenticating clients by using the MAC address of the client station as opposed to the user.

Network Address Translation (NAT)

The translation of one IP address used within a network to another address used elsewhere. One frequent use of NAT is the translation of IPs used *inside* a company, versus the IP addresses visible to the outside world. This feature helps increase network security to a small degree, because when the address is translated, this provides an opportunity to authenticate the request and/or to match it to known, authorized types of requests. NAT is also used sometimes to map multiple nodes to a single outwardly visible IP address.

Network Interface Card (NIC)

Generic term for network interface hardware that includes wired and wireless LAN adapter cards, PC Cardbus PCMCIA cards, and USB-to-LAN adapters.

Network Management System (NMS)

Software application that controls a network of multiple access points and clients.

Node

Generic term for a network entity. Includes a access point, network adapter (wireless or wired), or network appliance (such as a print server or other non-computer device)

Network Time Protocol (NTP)

NTP servers are used to synchronize clocks on computers and other devices. 108 Mbps Wireless APs have the capability to connect automatically to NTP servers to set their own clocks on a regular basis.

Ping Packet INternet Groper (ping)

A utility which determines whether a specific IP address is accessible, and the amount of network time (measured in milliseconds) for response. Ping is used primarily to troubleshoot Internet connections.

PLANEX Client Utility (ACU)

Application that executes on a client station and provides management and diagnostics functionality for the 802.11 network interfaces.

Policy-based Networking

The management of a network with rules (or policies), governing the priority and availability of bandwidth and resources, based both on the type of data being transmitted, as well as the privileges assigned to a given user or group of users. This allows network administrators to control how the network is used, to help maximize efficiency.

Power Over Ethernet (PoE)

Power supplied to a device by way of the Ethernet network data cable instead of a electrical power cord.

Preamble Type

The preamble defines the length of the cyclic redundancy check (CRC) block for communication between the Access Point and a roaming network adapter. All nodes on a given network should use the same preamble type.

Quality of Service (QoS)

QoS is a term encompassing the management of network performance, based on the notion that transmission speed, signal integrity, and error rates can be managed, measured, and improved. In a wireless network, QoS is commonly managed through the use of policies.

Remote Authentication Dial-In User Service (RADIUS)

A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize service or system access. RADIUS permits maintenance of user profiles in a central repository that all remote servers can share.

Radio Frequency (RF)

The electromagnetic wave frequency radio used for communications applications.

Roaming

Analogous to the way cellular phone roaming works, roaming in the wireless networking environment is the ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

Rogue AP

An access point that connects to the wireless network without authorization.

Secure SHell (SSH)

Also known as the Secure Socket Shell, SSH is a UNIX-based command line interface for secure access to remote systems. Both ends of communication are secured and authenticated using a digital certificate, and any passwords exchanged are encrypted.

Service Set Identifier (SSID)

The SSID is a unique identifier attached to all packets sent over a wireless network, identifying one or more wireless network adapters as “belonging” to a common group. Some Access Points can support multiple SSIDs, allowing for varying privileges and capabilities, based on user roles.

Secure Sockets Layer (SSL)

A common protocol for message transmission security on the Internet. Existing as a program layer between Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers, SSL is a standard feature in Internet Explorer, Netscape, and most web server products.

Simple Mail Transfer Protocol (SMTP)

Protocol used to transfer email messages between email servers.

Simple Network Management Protocol (SNMP)

An efficient protocol for network management and device monitoring.

SNMP trap

A process that filers SNMP messages and saves or drops them, depending upon how the system is configured.

Spanning Tree Protocol (STP)

A protocol that prevents bridging loops from forming due to incorrectly configured networks.

Station (STA)

An 802.11 capable device that supports only one 802.11 network interface, capable of establishing a Basic Service Set 802.11 network (i.e., peer-to-peer network)

Static IP Address

A permanent IP address assigned to a node in a TCP/IP network.

Subnet

Portion of a network, designated by a particular set of IP addresses. Provides a hierarchy for addressing in LANs. Also called subnetwork.

Subnet Mask

A TCP/IP addressing method for dividing IP-based networks into subgroups or subnets (compare with maskbits). Each triplet of digits in an IP address consists of 8 bits. To specify using a subnet mask, indicate the masked bits as an IP address. To specify the subnet in maskbits, count the number of bits in the prefix. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Temporal Key Integrity Protocol (TKIP)

Part of the IEEE 802.11i encryption standard. TKIP provides improvements to WEP encryption, including per-packet key mixing, message integrity check and a re-keying mechanism.

Traffic Class Identifier (TCID)

Part of the standard 802.11 frame header. The 3-bit TCID is used for mapping to class-of-service values.

Transmission Control Protocol/Internet Protocol (TCP/IP)

One of the most commonly used communication protocols in modern networking. Addresses used in TCP/IP usually consist of four triplets of digits, plus a subnet mask (for example, 192.168.25.3, subnet 255.255.255.0).

Transport Layer Security (TLS)

Protocol that provides privacy protection for applications that communicate with each other and their users on the Internet. TLS is a successor to the Secure Sockets Layer (SSL).

Trunk

In telecommunications, a communications channel between two switching systems. In a wireless network, a trunk is a wireless connection from one access point to another.

Type of Service (ToS)

Sometimes also called IP Precedence, ToS is a system of applying QoS methodologies, based on headers placed into transmitted IP packets.

User Datagram Protocol (UDP)

A connectionless protocol similar to TCP/IP, but without the same level of error-checking. UDP is commonly used when some small degree of errors and packet-loss can be tolerated without losing program integrity, such as for online games.

Virtual LAN (VLAN)

A local area network with a definition that addresses network nodes on some basis other than physical location or even whether the systems are wired together or operating using the same local equipment. VLANs are, on average, much easier to manage than a physically implemented LAN. In other words, moving a user from one VLAN to another is a simple change in software, whereas on a regular LAN, the computer or device would need to be connected physically to a different switch or router to accomplish the same thing. Network management software of some sort is used to configure and manage the VLANs on a given network.

Index